1986-12

A model for the development of an organization's information system (IS) security system

Boyce, Joseph George

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A MODEL FOR THE DEVELOPMENT OF AN ORGANIZATION'S INFORMATION SYSTEM (IS) SECURITY SYSTEM

by

Joseph George Boyce

December 1986

Thesis Co-Advisors: James M. Fremgen
Michael P. Spencer

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
DECLASSIFICATION / DOWNGRADING SCHEDULE	
PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
NAME OF PERFORMING ORGANIZATION val Postgraduate School	6b OFFICE SYMBOL (If applicable) Code 54
7a NAME OF MONITORING ORGANIZATION Naval Postgraduate Schhol	
ADDRESS (City, State, and ZIP Code) nterey, California 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
NAME OF FUNDING / SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)
9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

TITLE (Include Security Classification)
MODEL FOR THE DEVELOPMENT OF AN ORGANIZATION'S INFORMATION SYSTEM (IS) CURITY SYSTEM

PERSONAL AUTHOR(S)
yce, Joseph G.

TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
ster's Thesis	FROM _____ TO _____	1986 December	156

SUPPLEMENTARY NOTATION

COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Security; Controls

ABSTRACT (Continue on reverse if necessary and identify by block number)

This thesis addresses the development of a system to secure appropriately organization from some discernible threats posed by the presence, power, d applications of its computers. It presents a conceptual definitional amework for an information system (IS) security system. This framework nsists of the system's objectives environment; resources; components asks); and management. A generic development model is established to nstruct a security system within this framework. The model consists of anning, design, and implementation (installation, testing, and management) ases. Conclusions are drawn which present the continuing need for such a velopment process within an organization. The development model is nsidered sufficient enough to serve as a basis for the performance of curity system developments within a broad range of organizations.

DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified
NAME OF RESPONSIBLE INDIVIDUAL rof. Michael Spencer	22b TELEPHONE (Include Area Code) (408) 646-2623 / 22c OFFICE SYMBOL Code 54Xq

Approved for public release; distribution is unlimited

A Model for the Development of an Organization's Information System (IS) Security System

by

Joseph George Boyce
IS Auditor, U.S. Naval Audit Service
B.S., Widener University, 1974

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
December 1986

ABSTRACT

This thesis addresses the development of a system to secure appropriately an organization from some discernible threats posed by the presence, power, and applications of its computers. It presents a conceptual definitional framework for an information system (IS) security system. This framework consists of the system's objectives environment; resources; components (tasks); and management. A generic development model is established to construct a security system within this framework. The model consists of planning, design, and implementation (installation, testing, and management) phases. Conclusions are drawn which present the continuing need for such a development process within an organization. The development model is considered sufficient enough to serve as a basis for the performance of security system developments within a broad range of organizations.

TABLE OF CONTENTS

I. INTRODUCTION

> There are some occasions, though, when the most significant force in a year's news is not a single individual but a process, and a widespread recognition by a whole society that this process is changing the course of all other processes. That is why, after weighing the ebb and flow of events around the world, TIME has decided that 1982 is the year of the computer. It would have been possible to single out as Man of the Year one of the engineers or entrepreneurs who masterminded this technological revolution, but no one person has clearly dominated those turbulent events. More important, such a selection would obscure the main point. TIME's Man of the Year for 1982, the greatest influence for good or evil, is not a man at all. It is a machine: the computer. [Ref. 1:p. 16]

A. THE COMPUTER

This thesis was written within the context of how the computer is changing our society and the potentials for good and evil that result from such changes. Unlike other inventions that have been developed, the computer's impact is sometimes hard to discern. Except in recent years, with the increasing use of microcomputers, the computer has remained hidden behind concrete and glass enclosed walls in buildings of varying shapes and sizes. It seemed to remain a mystery to all but a select few. One only felt its presence in the stacks of paper that would come reaming forward at select times. Even now, as the emphasis has shifted toward widely dispersed processing, the full force of its power, presence, and impact remain obscured.

The essential power of a computer lies in its capabilities to process, sort, store, and communicate vast amounts of data at great speed and accuracy. Such power reflects the logical dimension of computers rather than their physical dimension. Unlike many great inventions of society, like the car, the presence of the computer is more logical than physical. As computer technology advanced from the first to the current generation, the physical dimension of the computer decreased. This surely resulted from advances in software and circuitry.

It has only been in recent years that the computer's power and presence have begun to permeate our society in ever more noticeable forms. Perhaps this "macro" permeation could be compared with Richard Nolan's "micro" or organizational level Contagion Stage (Phase II) of Data Processing Growth. [Ref. 2:pp. 115-126] Surely, computer technology has been initiated (Stage I). As to whether society has imposed sufficient controls (Stage III) over this growth is debatable and beyond the scope of

this thesis. However, the issue as to whether an organization within society has recognized the need for and imposed sufficient controls on the threats to its IS will be addressed.

As the power, presence, and applications of computer technology increase within our society, the issue as to whether such growth represents any threats could and should be raised. With prior technologies, when such threats were detected and assessed as to be material in nature, society responded with various "macro" controls such as laws, regulatory bodies, and reporting requirements. At the "micro" level of society, organizations have also faced the issue of a multitude of threats imposed by technological proliferations.

This research addresses the development of a system to secure appropriately an organization from some discernible threats posed by the presence, power, and applications of its computers. Therefore, more than just the security of its physical assets with economic values will be discussed. As will be addressed later, the issues are more complex than economic valuations. It is intended that the research will provide a generic model which could be used by an organization to address complex information systems (IS) security issues. The model will provide a useful framework which could be expanded, as needed, to meet organizational IS security requirements.

B. RESEARCH OBJECTIVES

The following are the thesis research objectives:

- To place the IS security issue within the broad context of society, organizations, and individuals.
- To provide a conceptual systematic definitional framework for IS security.
- To provide a generic development model which could be used to construct an organization's security system within the conceptual framework.
- To establish a basic understanding of the need for IS security.
- To provide a basis for further research on and enhancements to the points discussed in the thesis.

Four primary research questions will be addressed to accomplish the stated research objectives.

- What is the basic importance of IS security to society, organizations, and individuals? (Chapter II)
- What is an IS security system ? (Chapter III)
- What are the needs for IS security with an organization? (Chapters IV - V)
- How can an IS security system be developed? (Chapters IV - VI)

Each of the three research questions will be addressed in the subsequent chapters. Chapter II intends to provide background information concerning the present impact that the computer is having on our society. Some of the threats and implications posed by the impact will be discussed. Chapter III presents the conceptual definitional framework of an IS security system using a "systems approach". Chapters IV to VI provide a development model which could be used to construct an organization's security system within that conceptual framework. Finally, Chapter VII presents some conclusions concerning the development model and the future of IS security.

II. BACKGROUND

A tool is but the extension of a man's hand and a machine is but a complex tool. He that invents a machine augments the power of a man and the well-being of mankind. [Henry Ward Beecher]

Men have become the tools of their tools. [Thoreau, *Walden*]

A. THE ISSUE OF IS SECURITY

The issue of IS security is one that is inextricably tied to the proliferation, diverse and wide application, interconnectivity, and significance of computers within our society. As a result of these and several other factors, society has become more and more dependent on the use of computers. This dependency varies as one discusses the multitude of entities that comprise our society. The economic system, for example, appears to be substantially more dependent on computer technology than other systems. This is understandable when one considers that the first extensive application of the technology involved the accounting functions of businesses.

The extent of IS dependency can vary by whatever environmental sector or entity one wishes to discuss. Therefore, it may be useful to provide a means of classifying this variation. Such an approach was performed at the organizational level [Ref. 3:pp. 216-218]. However, it is necessary to expand this approach to present a more balanced view concerning IS dependency.

The dependency of IS to any organization of society can be defined in two dimensions, two states, and six levels. There are two dimensions in which to express IS dependency. First, operational dependency occurs when the entity critically relies on IS operational support but is not absolutely dependent on the uninterrupted cost-effective functioning of this support to achieve either short-term or long-term objectives. Generally, such support involves functional applications (accounting, personnel, etc.) and management planning and control (management information systems). In other words, an IS does not play critical role toward the achievement of the entity's mission. IS applications tend to be internally focused systems and are used for cost reduction or quality improvement purposes [Ref. 4]. There are no interfaces with suppliers, customers, and clients.

Second, strategic dependency exists when an IS plays a critical role in both operational support and toward meeting strategic needs. There is the assumption that strategic dependency also involves operational dependency. In addition to the internal focus of operational support, there is now a more external or environmental emphasis. The IS plays a stronger role in the accomplishment of strategic objectives. Suppliers, clients, and customers interact with the IS. This is intended to enhance the organization's products or services.

One means of measuring the dependency of an IS to an organization involves an estimation as to the time the IS could be down before essential business functions cease. One study found that the average time period in which essential company functions will continue following a data center failure ranged from two days for the financial industry to 5.6 days for the insurance industry. All industries had an average of 4.8 days. [Ref. 5:p. 24] Generally, there are two underlying causes of an organization's dependency on its IS. First, the automation of its processes on a large scale. Second, the integration of the automated processes. Such causes involve the extent to which an organization has automated it operational, management, and strategic planning processes and the integration of those processes. Other things being equal, the greater the current and anticipated extent of the automation and integration, the greater the level of IS dependency.

At any point in time, an organization can be in two states. First, the current state simply indicates the current level of IS dependency. Second, the planned state represents the IS applications under development. Applications could be designed to meet anticipated operational and/or strategic requirements.

Finally, IS dependency can be expressed in a multitude of levels. Each level is a combination of the two dimensions (operational and strategic) and the two states (current and planned). At any given point in time, an organization can be at only one of six levels.

- *Level 1.* Currently, the organization is strategically and operationally dependent. Applications that are under development are expected to maintain this posture.
- *Level 2.* Currently, the organization is strategically and operationally dependent on the IS. However, applications under development are dominated by maintenance work and non-strategic applications.
- *Level 3.* Currently, the organization is only operationally IS dependent. However, applications under development are expected to create operational and strategic dependency.
- *Level 4.* Currently, the organization is only operationally IS dependent. Applications under development are expected to enhance operational dependency only.

- *Level 5.* Currently, the organizations is not operationally or strategically dependent on its IS. However, applications under development are expected to create an operational IS dependency.
- *Level 6.* Currently, the organization is not operationally or strategically IS dependent. Applications under development are not expected to create either a strategic or operational dependency.

A full discussion of society's growing dependency on the computer would be complex. It is a multidimensional issue which cannot be properly addressed with this thesis. However, a limited discussion of how the computer has become infused within our society will be presented. For it is only when we have some perception of the impacts that computers are having, can we understand their criticalness. When such a perception is constructed, then the subject of IS security and its development can be discussed.

The impact of computers on our society can be expressed in four perspectives. First, physically there has been tremendous proliferation of computers throughout our society. Second, the logical perspective addresses the vast amount of data which is being processed, stored, and increasingly shared. Third, computer technology is being increasingly applied to a wide and diverse range of organizations, processes, professions, and functions within society. Finally, the application of computer technology has resulted in new threats to human values which have existed on this planet for centuries. Such threats lead us to question what we value, why we value what we value, how to value, what threatens what we value, and how to protect and manage what we value.

B. THE PHYSICAL PERSPECTIVE

There has been a physical proliferation of computers throughout our society. The proliferation has been such that there are now some 30 million computers in the nation [Ref. 6: p. 38]. Certainly a major contributing factor has been the growing popularity of microcomputers by government, business, and the general public. Approximately 17 million are now in U. S. homes and offices [Ref. 7:p. 68]. It is estimated that this number could grow to as high as 80 million by the end of the century [Ref. 1:p. 16].

C. THE LOGICAL PERSPECTIVE

Author John Naisbitt [Ref. 8:pp. 1-33] concludes that our Industrial Age Society has evolved into an Information Society. At the heart of this new society is the computer. There is a mass-production of information in the same way we used to mass produce automobiles. Certainly, the computer is the primary producer, storer, and

distributer of the information. However, Mr. Naisbitt makes a critical distinction between the two societies. In the computer age, we are dealing with ***conceptual*** space connected by electronics, rather than by physical space connected by the motorcar. The significance of this point can be emphasized by understanding the vast amount of data that is being processed, stored, and shared throughout our society.

The Federal Government, for example, has more than 27,000 mainframe computers and more than 100,000 desk top computers [Ref. 9:p. 52]. It accumulates, stores, processes, and distributes vast quantities of data on a diverse range of subjects. More than 2.5 billion records are maintained in 229 fully computerized files. [Ref. 10:p. 4] Of those, 43 files contain more than 500,000 records and another 1 billion are stored in 310 partially computerized and manual files. These records, combined with the more than 600 data banks operated by the states and the more than 1700 data banks operated by the cities and counties, provide governments with specific information on virtually every citizen [Ref. 11:p. 570].

There has been a tremendous growth in the interconnections of computers into networks and the availability of commercial on-line databases. An estimated 2,400 on-line commercial databases are available for public use. [Ref. 7:pp. 68-72] In a typical month, merchants will initiate 50 million VISA credit checks to 18,014 member banks through a high-speed authorization system then can approve payment in as little as one second. The Traveler's Insurance Corporation spent $300 million in the past two years to bring its 30,000 employees and 10,000 independent agents under the umbrella of an IBM system network. Currently, the company has 35,000 terminals and personal computers (PCs) connected to 18 mainframe computers. Each day 3.7 million messages pass through Traveler's 2 million feet of coaxial and fiber optic cables. [Ref. 7]

The electronic transfer of funds has taken on great significance in our society. We are increasingly seeing the transfer and storage of funds being accomplished in milliseconds via data communications circuits from computer to computer in the form of electronic pulses, bistable circuit states, and magnetic domains. [Ref. 12:p. 267] Our economy is becoming increasingly reliant on Electronic Funds Transfers (EFT) and the interconnections of computer systems. Traditionally, funds have been accounted for by the accounting system then physically stored in steel and concrete vaults. The transfer of these funds was physically accomplished by movement in armored cars, airplanes, and railroad cars. Also, funds have taken the physical form of paper checks, securities, notes, telegrams, letters, warrants, currency, and precious metals.

However, there has been an increasing shift toward electronic storage and transfer of funds. For example, a large commercial bank transfers $30 billion each day and the U. S. Federal Reserve Wire System turns over an amount of money equal to the national debt every four days. The four major fund transfer systems that the nation relies on transmit $309 billion per day domestically and $600 billion per day internationally. [Ref. 12]

The national telephone system provides the largest communications network [Ref. 5 : pp. 38-39]. It is controlled almost entirely by computer and connects 100 million homes and businesses through 1 billion circuit miles of wire, cable, microwaves, and satellites. Finally, firms like IBM are offering corporations the ability to share information and applications worldwide [Ref. 13:p. 2].

As indicated, vast quantities of data affecting people are being collected, processed, stored, and communicated throughout society. It is essential that this data isn't lost or stolen, contain no errors and omissions, and is not originated, stored, retrieved, or communicated without proper justification. Therefore, proper security must exist to ensure that such discrepancies can be avoided or minimized.

D. THE APPLICATIONS PERSPECTIVE

There have been a wide and diverse applications of computer technology throughout our society. Such applications are more visible and publicized in the business community. However, computer technology has been increasingly applied to some significant and critical areas of society. Three such areas will be discussed.

1. The Political System

The entities of the nation's political system have been experiencing increased applications of computer technology to their tasks. As the dependency levels of these entities increase, so will be the need for greater protection over the information system that are applied.

The legislative bodies of our nation have been using various IS to support their operations. The Congress uses a system called LEGIS to record, store, and provide prompt computer response to inquiries about the current status of all bills and resolutions. [Ref. 11:p. 606] The SOPAD system enables members to receive up-to-the-minute summary of proceedings and debates taking place on the floors of the House and Senate. Also, FAPRS (Federal Assistance Program Retrieval System) helps members to determine what federal grants and loans can be used by their constituents.

State legislatures, such as those in New York, Washington, Florida, Pennsylvania, Hawaii, and North Carolina, make effective use of computers to index, store, process, and retrieve statutory material; draft bills; prepare roll-call vote reports; provide census population data for planning purposes; address mailing labels; and provide other information and services to legislators and their staffs.

Computer technology has also been applied to the Judicial System. An advanced computer-aided transcription (CAT) technology has been used by courts in Chicago, Phoenix, and Detroit. [Ref. 14:pp. 1 & 22] It serves to translate testimony in real-time and display it on video monitors in courtrooms. Also, this on-line CAT system provides attorneys with the ability to search for and retrieve specific portions of transcripts and provides fully edited transcripts within minutes after a court session.

CAT is of great benefit in those instances when witnesses or counsel do not articulate well enough to be understood by all parties. The real-time transcription enables deaf attorneys and litigants to read testimony they could not hear. The most significant advantage for attorneys is the ability to receive daily transcripts on computer disks, ready for indexing and cross-referencing on microcomputers. As a result, information is quickly accessible and more easily researched using the CAT.

Additional application to the judicial system may result. There will eventually be automated statute and precedent research. Also, telecommunications will enable the transmission of trial information to the attorney's office the instant it has been converted to text. This would permit greater time to perform research for subsequent court sessions.

2. **Journalism**

Journalists have found the computer an effective tool for discovering information which would have "... remained buried like a treasure crest at the bottom of the sea". Computer technology permits archival scanning that once required exhaustive card-catalog searches and high-speed analysis of myriad numbers until the machine produces a revelatory pattern. Several examples follow. [Ref. 15 :p. 56]

The computer was used to analyze 30,000 low-interest mortgages issued by a mortgage finance corporation. The journalists matched mortgage issue dates with the bond issue that financed them. These helped expose a "secret fund" that apparently was used to give out loans to politically connected people. Criminal indictments resulted from the investigation.

One reporter heard that undefended indigents were being jailed for months because they could not pay $100-to-$300 fines for offenses like jaywalking. Records of 899 inmates were fed through a computer. As a result of this analysis, the courts freed hundreds of inmates, threw out 20,000 orders for jail commitment and told the county to provide attorneys for poor defendents. It was estimated that without the computer analysis, the work would have required up to a year of research rather than six weeks.

In 1979, a newspaper scanned with a computer all 2 million of a county government's property-tax assessments to discover inequities. In 1984, another newspaper used the computer to examine every state-awarded highway contract in the area and all major county sewer contracts over eleven years to discover that five favored firms collected 86% of the awards. The application of computers in journalism will continue to be significant as more and more public data are processed using computers.

Therefore, the issue of IS security becomes significant for two reasons. First, there needs to be a means of determining what is public information and procedures established for accessing it. Second, the integrity of stored public information needs to be maintained to ensure that what may be publicly stored and reported is valid. [Ref. 15]

3. **Monitoring, Control, and Decision Making**

The public and private sectors have been increasingly using computers to monitor, control, and decide on a variety of activities. Such activities include such areas as weather forecasting, national defense, work performance, medical care, and the stock market. Therefore, the protection of the IS designed for such functions is becoming increasingly important.

The government and industry have been increasingly using computer technology to monitor and control a variety of activities. The Internal Revenue Service has applied computers to monitor the returns of individual and corporate taxpayers. [Ref. 11:p 607] The reports of interest paid by banks to individuals can be compared against income reported by the taxpayer. Also, computers are used to select randomly and make preliminary audits of tax returns.

Environmental control has been another area of application. U. S. governmental agencies processing environmental data with the assistance of computers include the Air Pollution Control Office and the Water Quality Office of the Environmental Protection Agency, the National Center for Health Statistics, the U. S.

Geological Survey, and the Department of Agriculture. At the state and local governmental levels, computers are being used to evaluate and control the levels of pollution. A significant result of the application of computer technology to meteorology has been the ability to predict hurricane paths. [Ref. 16: pp. 3 & 5] It is now possible for meteorologists to predict fairly accurately the circuitous paths hurricanes will follow and thus reduce the potential damage and loss of human life.

The Department of Defense (DOD) has developed the World Wide Military Command and Control System for U. S. military commanders from the President on down. [Ref. 11:pp. 277-278] This system links 35 large computers at 26 command posts around the world. The computers at the North American Air Defense Command accept, store, and constantly update masses of data from worldwide radar installations. The system can also track every humanly produced object in earth orbit. On the civilian side, millions of aircraft flights are monitored across the nation each year by the computers of the Federal Aviation Administration 's (FAA) Air Traffic Control System.

Computers are being used to monitor the work performance of the people who use them. [Ref. 17:p. 46] It is estimated that 13 million Americans use computer terminals in their work, and about one-third of them are being monitored by the computer as they work. The computer is programmed not only to process information from each employee's terminal but also to measure, record, and tabulate dozens of details about how efficiently the worker is utilizing the system. Airline-reservation computers, for example, closely measure how long individual clerks take to handle each customer, and the amount of time the employee spends between calls. Any idle time is recorded, as well as lunch hours, coffee breaks, and even trips to the bathroom.

Computer technology has made significant contributions to the quality of medical care. In some hospitals, for example, patients are able to sit down at a computer terminal before meeting a doctor to provide their medical histories and to receive information about the hospital. [Ref. 18:pp. 47-48] The computer interviews can be done in several foreign languages, as well as English, with a doctor receiving an instantaneous translation. Information on some ailments, such as stroke and blood disease, has been computerized within the hospital for doctors' consultation. Currently, computers have the capability of detecting and monitoring ocular and cerebral ailments such as glaucoma and brain tumors. Some hospitals program computers not only to remind the pharmacy department to prepare prescriptions but also to alert nurses to

give the proper dosage at the right time. A patient's medical history can be updated with the use of terminals located throughout the hospital. More broadly, computers permit the patient to be able to receive a health profile at far less cost than previously possible; and by systematizing information about the patient, reduce his or her hospital stay and pare both institutional and patient cost.

Another significant accomplishment in the health care field has been the establishment of medical detecting and advising systems. [Ref. 19] Such systems are accessible to hospitals located throughout the nation. As patient's are examined, medication orders and test results are entered into the system. The system contains data relative to various symptoms and the advised medications. Also, the patient's medical history is contained within the system's data. The history includes the patient's record of examinations; history of ailments; the doctor's and nurse's notes; data from monitoring equipment, such as electrocardiograms; and, from laboratory test machines, such as an automatic blood analyzer or X-Ray machine. As data is input, the system analyzes it and immediately begins asking for more information, suggesting tests, offering a diagnosis or reacting to the doctor's treatment plan by warning of drug interaction, patient allergies or other potential problems. In one system, Control Data Corporation's Health Evaluation through Logical Processing (HELP), the doctor doesn't have to take the computer's advice. However, the reason for this must be explained in the patient's record by the doctor. HELP acts as a flexible checklist for doctors. The system is programmed to react to the changing conditions of the patient as a disease progresses or as new laboratory tests or other information becomes available.

Finally, computers are playing an increasingly significant role in the buying and selling of stock. First, the New York Stock Exchange uses 13 computers to support minute-to-minute floor trading. [Ref. 20:p. 10A] It is estimated that if three of the computers fail, stock trading would cease. Second, large investors are using computers to monitor stock prices and to sell or buy automatically when they reach a particular point. [Ref. 21:pp. 1B - 2B] This " program selling " is dominated by a few major Wall Street brokerages. Third, the nation's stock exchanges have applied computer technology to enhance their abilities to monitor and control illegal activities related to stock trading. [Ref. 22:p. 46] The New York Stock Exchange (NYSE), the American Stock Exchange, and the Over-the-Counter NAS-DAQ Systems employ comprehensive computer systems to monitor unusual stock trading. In 1985, the NYSE

instituted an audit trail allowing it to track the buyers and sellers involved in each trade.

E. THE VALUE PERSPECTIVE

Ultimately, the question of values and the threats to and the limitations on those values imposed by the increasing use of computer technology must be addressed. Traditionally, such issues tended to focus more strongly upon the physical and application perspectives of computers. The security issues involved protecting computer systems as assets with economic value. Also, applications should contain sufficient controls to prevent malfunction, error, damage, destruction, or fraud which could result in the loss of economic and human values.

However, as previously discussed, the power of the computer system is no longer defined by its size and limited applications. The logical power of a computer in terms of processing, storage, and communications has reached a point of dominance. As a result, the issues of what we value as a society and the threats to those values take on a broader context.

1. Human Privacy, Freedoms, and Power

First, human privacy, freedoms, and power are threatened by the increasing mass processing, storage, and communication of information. Vast amounts of information on individuals are stored in a number of private data banks. [Ref. 23:p. 104] The data is sold to businesses and individuals for a designated price. Computer "blacklists" of consumer information are sometimes used as a basis for denying housing and credit to consumers on the list.

Credit bureaus such as TRW Information Services and Equifax, Inc. have long relied on huge data banks of mainframe computers to provide consumer credit records for banks, department stores, finance companies, and employers. Each working day, TRW's machines handle an average of 255,000 requests culling information from a massive data base that contains detailed records of the bill-paying habits of 133 million people.

Our society established controls in the form of laws. Under the Federal Privacy Act of 1974, for example, the Census Bureau, the Internal Revenue Service (IRS), and other government departments must notify citizens before releasing information about them to another agency. Consumers also have the right to stop credit bureaus from dispensing false or misleading data. However, the regulations governing the new private blacklists are murky and contradictory. [Ref. 23]

Also, a congressional investigation concluded that advances in technology are eroding the Federal Government's ability to ensure privacy of personal information stored in government computers [Ref. 24:pp. 1 & 14]. The Privacy Act of 1974 was developed under certain technical and social conditions. [Ref. 25:p. 60] Batch processing was dominant in 1974 and government agencies and large businesses were the major users of computers. Also, the telecommunications industry was regulated and highly structured. Its development and functioning were mainly separate from computer systems.

The technological changes that have taken place over the last 12 years were not provided for in the act. For example, there has been an increase in modem (the device used to link a computer with a network) capabilities nationwide. An estimate by the U. S. National Security Agency (NSA) indicated that all the modems purchased in the U. S. in 1972 could together transmit 600,000 characters per second. However, in 1984, a sufficient number of modems were purchased to transmit 220 million characters per second. With the increase in quantity of transmission has come an increase in speed. The Office of Technology Assessment (OTA) estimates that with the increased communications capacity made possible by fiber-optics, it is possible to transmit at a rate of 100 average-length pages per second. This capability could permit the creation of centralized libraries with universal access. [Ref. 25]

The growth of computer technology challenges the balances of power within our society. These balances exist between man and machine as well as between men who apply computer technology. The balance of power between man and machines essentially involves two issues. First, the extent to which man permits computers to monitor and control human and non-human activities such as in work performance monitoring. Second, the extent to which man permits computers to actually decide critical questions without human intervention. This second issue has great relevance in the areas of health, economics, and national defense.

When computer technology is applied to various aspects within our society it sometimes alters or threatens to alter the existing power balances. The machine can be used as an instrument for shifting the balance of power beyond safe limits. For example, the governor of the state of New Hampshire reorganized the state's computerized financial management system. [Ref. 26:p. 70] He established an integrated financial management system which reported state budgetary, revenue, and expenditure information. As governor, he freely accessed the system to obtain required information.

However, the issue of the availability of the data was raised by the state legislature. The governor attempted to retain control over who could access the stored data. This was perceived as an attempt to try to shift control from the legislature to the governor's office. However, the governor did agree to issue a password to one legislative official under certain limitations. Only limited information from the system could be accessed by the legislature. The state's computer contains revenue, expenditure, budgetary, and operational information. Such information provides a basis for managing the government; assessing its performance; and making decisions in these areas. If the legislature's access to such information is narrowly restricted by the governor, then it may not be able to properly perform its duties. Such duties include assessing the state's financial and operational performances and making sound decisions that it is constitutionally empowered to make. At the time of this writing, the matter has not been resolved. However, this case illustrates the political implications that could result from the application of computer technology in an organization.

2. **Human Vulnerability**

Society is becoming increasingly vulnerable to computer system destruction, damage, malfunctions, errors, misuse, and fraud. As previously indicated, this results from the expanded proliferation, power, and applications of computer technology within the society. It is estimated that the overall losses to U. S. businesses from computer crime are from $100 million to $3 billion annually [Ref. 27:p. I-1-4]. In the public sector, government computer disorders have been estimated to result in annual losses of $30 billion to the American taxpayer [Ref. 9].

The vulnerability of our society can also be expressed from an operational perspective. Computer systems eventually become integrated with the other systems of an organization and society. As discussed earlier, this integration could reach a point where organizations become dependent to varying degrees on the computer to accomplish operational and strategic objectives. As the degree of integration increases, the levels of operational and strategic dependency of the organization also increase. Therefore, the various systems within our society and organizations become increasingly vulnerable to computer destruction, modification, disclosure, and denial of service.

The scope of this vulnerability could extend from a single individual to the entire human race. Certainly one system which has global significance is our national security system. Its existence and readiness secures mankind from Armageddon. This

system has become increasingly dependent upon computer technology to maintain that readiness. A clearer picture can be presented of the vulnerability issue when one considers that a study revealed that only 30 out of about 17,000 DOD computers surveyed met minimum standards for protection [Ref. 28:p. 39].

F. CONCLUSIONS

It is hoped that this chapter offered some insight into the broad or "macro" perspective of computers and the need for some degree of control over them in various circumstances. Due to the scope of this thesis, it was not possible to explore the presented issues in any greater depth. However, it is within this "macro" perspective that an IS security system must be developed to meet threats at both the "macro" and "micro" or organizational levels. As society's dependency on computer technology has increased, it has responded with controls in the form of laws, regulations, and regulatory bodies to counter the threats. So too must individual organizations respond with controls as its level of dependency and threats rise. An orderly process should be followed by organizations to assess its security needs and to select appropriate controls to meet those needs. The development of such a process is the subject of this thesis. The following chapter will address the definition of an IS and an IS security system.

III. THE SYSTEMS PERSPECTIVE

The whole is more than the sum of its parts. [Aristotle]

A. WHAT IS A " SYSTEM " ?

1. System Definition

Generically, a system can be defined as a set of parts coordinated to accomplish a set of goals. It is possible to conceive of a hierarchy of systems which encompass the entire universe. Man has developed political, economic, technological, social, and legal systems to enable him to survive, coexist, and prosper. Within each of these systems, other systems (organizations) were formed over time through the combination of people, resources (time, currency, energy, materials, equipment, space, information, and technology), procedures, structure, and goals. These organizational systems are embedded within the universal system. There are five basic considerations that one must keep in mind when thinking about the meaning of a system. [Ref. 29:pp. 29-47]

First, each system must have total objectives and means to measure the performance of the whole system. A distinction needs to be made between a system's stated objectives and the real objectives. Some objectives may be publicly stated to accommodate groups and win support. Such a situation could arise to obtain a larger budget, win customers, or obtain investment funds. A means of separating real and stated objectives is to determine whether the system will knowingly sacrifice other goals in order to attain the stated objective. Once measures of performance are developed to assess the accomplishment of the objectives, a distinction should also be drawn between stated and real measures of performance. For example, a student in class often comes to think of his or her objective as the attaining of as high a grade as possible. The measure of performance becomes the letter grade obtained when the course is completed. Such a high grade could be achieved at the sacrifice of a real understanding of the content of the course. The high grade is sought because he or she believes that high grades will lead to scholarships and other opportunities in the future. The student's stated purpose is to learn but his or her real measure of performance is the grade.

Second, the system's environment needs to be considered. The environment lies "outside" the boundaries of the system. Physical boundaries do not define what is "inside" and "outside" the system. The environment represents constraints on the system. The system can do relatively little about the environment's characteristics or its behavior. In effect, the environment is beyond the control of the system but it is also something that partly determines how the system performs. For example, if the system is operating in a very cold climate, then the equipment must be designed and protected to withstand various kinds of severe temperature changes. An important aspect of the environment of the system is the "requirement schedule". For an industrial firm, this consists of the sales demands. These demands could be somewhat influenced by means of advertising, pricing, and the like. But to the extent that demand for the organization's products is determined by individual people outside who are the customers of the firm, then the demand lies in the environment of the system.

Internal resources comprise the third relevant element of a system. Resources represent the things the system can change and use to its advantage. Such resources include people, currency, energy, materials, space, time, information, technology, and equipment.

Fourth, a system consists of components and their relevant goals, activities, and measures of performance. Generally, organizations are divided into departments, divisions, offices, and groups of individuals. These represent the structures that will perform the components (tasks). They may not represent the real components of the system but rather the stated ones. A department or unit may not perform just one task such as production. Rather it may perform several tasks. Therefore, there needs to be a rational breakdown of the tasks the system must perform. An analysis of the tasks will permit an estimate of the worth of an activity for the total system. If a department or other organizational subdivisional is associated with several larger tasks, it may be impossible to distinguish its real contribution. It must be determined if the departments and other subdivisions are relevant to the real components of the system. The components (tasks) whose measures of performance are truly related to the measures of performance of the overall system must be discovered.

Fifth, system management generates plans for the system - goals, environment, resources, and components. It sets the component goals, allocates the resources, and controls the system's performance. [Ref. 29:pp. 29-47]

2. System Thinking

The five elements just discussed must satisfy the following three conditions. [Ref. 30:pp. 2-3]

- The behavior of the whole is affected by the behavior of each of the five elements.
- There is an interdependency between the behavior of the elements and their effects on the whole system.
- Regardless of how the subgroups of the elements are formed, each has an effect on the behavior of the whole and none has an independent effect on it.

Therefore, a system is a whole entity that cannot be divided into independent parts. Two of a system's most important properties are derived from this statement:

- Each part or element of a system has properties that it loses when separated from the system.
- Every system has some properties - its essential ones - that none of the parts have alone.

The essential properties of a system taken as a whole result from the interactions of its parts or elements, not actions taken separately. As a result, when a system is taken apart (analysis) it loses its essential properties. Due to this critical fact, a system is a whole that cannot be understood by analysis. [Ref. 30:pp. 2-3]

Therefore, a method other than just analysis is required for understanding the behavior and properties of systems. System thinking involves the reversal of the the three-stages of Machine Age thinking : (1) decomposition of that which is to be explained, (2) explanation of the behavior or properties of each part separately, and (3) aggregating these explanations into an explanation of the whole. Analysis (taking things apart) is the critical factor in the process. Synthesis (putting things together) is used as a means of putting together behaviors and properties in a meaningful way. System thinking views these two means as inseparable. [Ref. 30]

System thinking is a process involving the following:

- Identification of a whole of which the thing to be explained is a part.
- Explanation of the behavior or properties of the whole.
- Explanation of the behavior or properties of the thing to be explained in terms of its role(s) or function(s) within its whole.

Using this approach, synthesis precedes analysis.

In analytical thinking, the thing to be explained is regarded as a whole to be taken apart. Synthetic thinking regards the thing to be explained as a part of a containing whole. In effect, analysis focuses on structure and reveals how things work. Synthesis concentrates on function by revealing why things operate as they do. As a result, analysis yields knowledge and synthesis yields understanding.

B. WHAT IS AN INFORMATION SYSTEM (IS) ?

An IS is conventionally defined as information resources plus all users of the information. [Ref. 31:p. 2] Information resources consist of all the physical and logical components of the IS such as computers, programs, analysts, programmers, operators, managers, data, operating systems, and communications links. The physical, logical, and human elements of the IS can be structured in the "system" conceptual framework previously discussed. A more comprehensive and structured definition will prove useful for formulating and implementing an IS security system.

1. IS Objectives

Information is the basic requirement of IS users. It can be delivered to users in physical (hardcopy) and logical (terminal display and voice outputs) forms. Generally, users have specifications for receiving the information. These specifications involve the information format; timeliness; cost; storage; availability; reliability; volume; distribution; and protection.

The prime objective of the IS is to meet user requirements (demands) for information relative to their specifications. The measures of performance for the IS involve criteria to assess the effectiveness and efficiency of the IS in satisfying user demands. If the IS plays a strategic role in the accomplishment of the organization's objectives, then such measures will also include criteria for assessing the performance of the users, or their organizational units using the IS for accomplishing their organizational missions. [Ref. 32:pp. 57-58]

2. The IS Environment

The IS environment consists of four elements. First, there is the environment outside the organization within which the IS is embedded. This environment is relevant to the IS since it produces the technology, products, and services which are utilized by the IS to perform its mission Also, this environment is responsible for producing the laws, regulations, and standards which affect the behavior of the IS in performing its activities.

Second, the top management of the organization provides the funding, direction, and commitment needed to support the IS. It affects the behavior of the IS by controlling the intensity levels of the three variables. Such intensity could range from high to low depending on the organization's level of dependency on the IS. A high level of dependency would require a high level of funding, commitment, and direction in terms of the products and performance it requires from the IS.

A third factor is the line, support, and general management components (tasks) and structures of the organization. The IS is responsible for providing information to these components (tasks) and the structures that are formed to provide such components (tasks). Organizational components (tasks) would include line (e.g., production, marketing, and engineering); support (e.g., accounting, administration, and purchasing); and general management (e.g., strategic planning, capital budgeting). The structures formed to perform such tasks include departments, divisions, sections, groups, staffs, and offices.

Fourth, the IS has various types of users of its products, services, and resources. Such users are people within and outside (e.g., suppliers, customers, and dealers) the organization who are authorized to receive information produced by the IS and to utilize its resources. Top management personnel are included as those who receive IS products and services as well as utilize IS resources. Consumers are users who are authorized to receive IS products and services and to utilize the IS resources. Owners are users who have exclusive rights and use over IS products, services, and resources. IS resources (hardware and software) are generally owned by the IS. Information, however, is generally owned by the organizational components (tasks) and structures (e.g., accounting, marketing, production). In a decentralized or distributed IS configuration, resources could be owned by the consumers. Custodians are users who are responsible for IS products and resources while they are under their possession. For example, service bureaus and time-sharing services operate on a third-party contractual basis. [Ref. 33:p. 3A-5]

3. IS Resources

There are seven types of IS resources. First, IS facilities include physical plant and supporting equipment and utilities. Second, IS technology can be either batch or on-line. Batch technology involves the processing of a number of similar input items which are grouped for processing during the same machine run. There is no interaction between the users and the job while it is processing. On-line technology involves the processing of data as it is generated. Interaction between the user and the job while it is running can take place. Third, hardware consists of units such as central processing units; magnetic storage devices; input/output devices; communication controllers; modems; terminal concentrators; digital switches; cryptographic devices; and multiplexors. A fourth IS resource is software. Software involves operating systems; database management systems; communications control software; and applications

software. Fifth, the data resource can be divided into various groups such as accounting, proprietary, and personal information. Sixth, people are the individuals who develop, operate, and manage the IS. Finally, procedures are the standards, rules, and policies established to develop, operate, and manage the IS.

4. **IS Components**

There are twelve IS components (tasks). Some or all of the IS resources are combined to construct each of the twelve components (tasks). In other words, the data entry component (task) could involve hardware (terminals); people (data entry personnel); procedures (data entry manual or users manual); and data (invoices). The combination of these resources forms a component or IS task. Such components (tasks) involve data origination, collection, preparation, and authorization; data input; data processing; data output; output distribution; storage & retrieval; communications; data management; hardware operations; system programming; application program maintenance; and system development. A organization may have all or part of these components (tasks). For example, a centralized IS configuration may not have a communications component (task) if all input documents are mailed or delivered to the IS for processing. Generally, the higher the level of IS dependency, the more of these components (tasks) an IS will contain.

5. **IS Management**

There are several aspects to the management of an IS. First, the mission of the IS needs to be established. This mission should be a reflection of the information needs of its environment. Second, a short range (1 year or less), intermediate range (1 to 5 years), and long range (greater than 5 years) strategy needs to be formulated to accomplish the designated mission. Such a strategy consists of overall and component objectives; measures of performance; application developments; policies; procedures; processes; and rules. It is through such a strategy that the people within the organization perform the activities needed to fulfill the mission.

Third, IS resources will need to be allocated to components to develop and maintain classes of IS applications. These classes of applications include transaction processing systems (TPS); management information systems (MIS); decision support systems (DSS); office automation systems (OAS); strategic information systems (SIS); and communication systems (local area networks and wide area networks).

An application can be defined in two ways. One way involves an organization's structural components (tasks). Such applications support general

management, line, and support components (tasks). The other way to define an application is in terms of its application to various fields of study such as medicine, science, military, education, and law. The application systems within the classes are developed and maintained over time to fulfill user requirements.

Fourth, resources, components, and management activities need to be structured and deployed. There are three configurations that are generally utilized. [Ref. 34:p. 16] A centralized configuration entails all data processing and storage capabilities at one geographic location, possibly with nonintelligent (non-data editing or local storage capabilities) terminals, either batch or interactive on-line, at other geographic locations. On the other hand, independent components and resources in different geographic locations which do not communicate are considered a decentralized configuration. A distributed configuration entails resources, components, and management in different geographic locations which communicate and process applications cooperatively.

C. WHAT IS AN IS SECURITY SYSTEM ?

1. Security System Objectives

The basic objective of the IS security system is to provide protection for the organization's IS physical (facilities, hardware, and procedures), logical (software and data), and human (people) assets. IS assets are to be protected from a variety of threats which could cause modification, destruction, disclosure, and denial of service of the assets. The measures of performance for the security system involves how effectively and efficiently the assets are protected from the threats which could cause such adverse impacts.

2. The Security Environment

The IS security system's environment consists of three factors. First, there is the environment outside the organization. This environment is relevant to the security system since it produces the technology, products, and services which are used by the security system. It also produces the laws, regulations, and standards which affect its behavior and objectives.

Second, the top management of the organization provides funding, direction, and commitment which is needed to support the security system. It affects the behavior of the security system by varying the intensity of these three variables.

Third, the IS security system is embedded within the IS of an organization. Although the security system operationally functions within the IS, it is separately managed by the security staff.

3. **Security Resources**

The security system's resources are controls in the form of security hardware, software, people, procedures, and data. The security controls such as security manuals; guards; separation of duties; passwords; hardware terminal locking; and restricted dial-up access are applied to IS resources. The controls provide the means of linking or operationally embedding the security system within the IS.

4. **Security Components**

There are six components (tasks) of the security system. First, the avoidance component (task) seeks to avoid threats to assets by removing the potential threat or by eliminating or moving assets away from potential threats. An example would involve removing a sensitive data file from on-line access during periods of time when potential threats are present. This situation could arise during hardware maintenance or time-sharing by unknown individuals.

Second, the deterrence component (task) involves activities to reduce the threat to assets by reducing the vulnerability of the assets to loss. An example would include labeling all copies of computer programs, data, computer equipment documentation, and storage media with warning labels. Such a label could read "Unauthorized modification, destruction, disclosure, taking, or use is punishable by law".

Third, the prevention component (task) involves reducing the frequency with which causes of threats occur. Examples include segregation of duties; passwords; authorizations; and standardization.

Fourth, the detection component (task) involves the notice of an attempted or actual threat. Examples include control logs; fire detection; hardware checks; operator logs; and operating system checks.

Finally, the recovery and correction components (tasks) involve activities which support the restoration from and replacement of loss. Examples of such activities involve the development of contingency plans; off-site back-up; on-site backup; and discrepancy reports. [Ref. 12:pp. 299-309]

5. **Security System Management.**

There are several aspects to the management of an IS security system. First, the management of the system is responsible for the establishment of the mission or objectives of the security system. This mission or objective(s) should be a reflection of the security requirements of the security system's environment.

Second, short range, intermediate range, and long range strategies need to be formulated to accomplish the designated mission. Strategies consist of overall system and component objectives; measures of performance; policies; procedures; processes; rules; standards; budgets; and reviews and evaluations. It is through such strategies that people within the organization perform the activities needed to accomplish the mission.

Third, appropriate security resources (controls) should be allocated to IS resources to ensure their protection. Such controls take the form of devices, procedures, and people.

Finally, security system resources (controls), components (tasks), and management should be structured and deployed within the organization. There are two appropriate configurations. One involves a centralized concentration of security resources (controls), components, and management. This would reflect a centralized IS configuration. The other approach involves a more decentralized structure and deployment of security resources (controls), components (tasks), and management. Such a configuration would reflect a decentralized or distributed IS configuration.

D. WHAT IS THE IS SECURITY SYSTEM DEVELOPMENT MODEL ?

A major objective of this thesis is to provide a conceptual systematic framework for defining IS security. This chapter defined an IS security system in terms of its objectives; environment; components (tasks); resources (controls); and management.

The other major objective is to provide a generic development model that could be used by an organization to construct a security system within this defined framework. Chapters IV to VI are intended to provide an orderly process for constructing and maintaining the security system. The development model consists of three phases. Each phase will produce various parts of the security system.

The planning phase will address the development of a security system development plan; a definition of the responsibilities for IS security within the organization; the establishment of security baseline requirements; the classification of

IS applications, data, and transactions; and the establishment of a security policy for the organization. The planning phase will produce the security system objectives and environment parts of the security system framework.

The design phase is responsible for producing the security resources part of the security system framework. Security resources are the controls which should be applied to the IS resources to provide the required level of security based on the classification performed during the planning process. The security controls effectively link the IS with the IS security system.

Finally, the implementation phase will involve the testing of selected security controls; the installation of the controls; and the development of a management structure and components (tasks) to manage the security system to ensure that the security objectives are accomplished. This phase will produce the components (tasks) and management parts of the security system framework.

IV. THE PLANNING PHASE

I like the dreams of the future better than the history of the past. [Thomas Jefferson, Statesman]

I never think of the future, it comes soon enough. [Albert Einstein, Scientist]

A. INTRODUCTION

There are five steps of the planning phase of the IS security system development process. First, an organizational security system development group will need to be formed. This group will have prime responsibility for formulating security objectives and priorities. Also, they are responsible for managing the planning, design, and implementation phases of the development process. Second, the responsibilities for IS security will be defined for the organization's top management, line management, and the IS security staff. Third, IS security policy will be formulated. This policy will consist of both security objectives and security priorities. Fourth, the IS security environment will be both defined and analyzed. The purpose of this analysis is to establish the organization's baseline security requirements. Finally, a security classification program will be established. The purpose of this program will be to classify IS applications, data, and transactions as to their criticalness and sensitivity. This will provide a basis for the allocation of security controls during the subsequent design phase. The planning phase will also begin the accumulation of relevant security information in an IS security database. Once the information is fully accumulated at the end of the development process, the database will provide a means of maintaining and managing the developed security system.

B. SECURITY SYSTEM DEVELOPMENT GROUP

1. Development Group Members

There are two approaches for staffing the development group. The first approach involves forming a group consisting of representatives from functions that relate to IS security. This group could work on a full-time basis or they could allocate limited number of hours per week to the development effort. Such functions include IS operations; hardware maintenance; systems programming maintenance; systems

development; quality control; IS standards; application programming; users; database administration; facilities management; general security department; the legal staff; personnel department; and the fire department.

Each representative must function in the group in isolation from representatives of all other functions requiring security. This enables a separation of responsibilities and maintains the principle of privilege or need to know. An example would illustrate the point. It would be unwise to have a programmer studying operations security. The separation of responsibility is a significant organizational control. Each assigned representative must be able to devote significant time to the group. Such an undertaking requires fixed schedules of work for the group and well-planned and coordinated meetings, especially to maintain the necessary separation of responsibilities. To accomplish this, the group will require a commitment from the organization's top management.

The second approach for the formation of a development group is to staff the group with IS security specialists augmented by individuals having whatever additional expertise is required. The security specialists would work on the development on a full-time basis. Also, if additional expertise cannot be obtained within the organization, then contractual relationships could be established with outside consulting services. [Ref. 35:pp. 107 - 111]

Each approach offers both benefits and disadvantages. Certainly, the use of representatives from a broad range of functions would provide greater knowledge, skills, and ideas. However, the representatives would not be available to serve in their normal capacities while participating in the security system development. Also, there is always the possibility that by exposing critical IS security information to a wide group of people, there is a greater risk of intentional or accidental disclosure.

The use of IS security specialists provides the benefit of specialized knowledge and limited exposure to critical security information. However, there may be a cost of additional development time since the specialists will need time to become familiar with the IS and the organization. Regardless of which approach is taken, an IS security manager should be appointed and given the leadership of the development group. Finally, the group should contain representatives from both the organization's and the IS top management.

2. Development Group Responsibilities

The development group will have overall responsibility for the planning, design, testing, and implementation of the security system. The security staff will be responsible for the system's management and operations.

The group's responsibilities will include the formulation of a security system development plan and procedures for monitoring the progress of the plan. Such monitoring will include periodic meetings, personal observation's, and the creation and distribution of periodic reports. Estimates of security system staffing; funding; development time; and management commitment and direction should be developed.

C. DEFINITION OF SECURITY RESPONSIBILITIES

1. Background

First, there must be a definition of management responsibilities for IS security. [Ref. 27:pp. I-1-6 to I-1-8] IS security is a management responsibility. Each organizational level must be responsible for the protection and conservation of its assigned resources. IS security is a basic function of management control at each level within the organization.

2. Top Management

It is the responsibility of top management for making the initial commitment to establish an IS security system within the organization. Also, top management has the continuing responsibility for providing a responsible and responsive managerial climate for the system's implementation and operation. Such a commitment should initially manifest itself in a clear and unambiguous statement of organizational security policy and continue in the form of high managerial visibility and concern with the effectiveness of the system.

3. Line Management

The ultimate responsibility for the protection of IS resources must rest with those who utilize or allocate the resources. Midlevel and first-line managers and supervisors are well positioned to identify those areas which require protective measures and to implement (or request implementation of) such measures. At this level, responsibilities for IS security involves the three distinct groups of users previously identified. First, IS consumers have three responsibilities as follows:

- Ensuring that IS assets are used only for authorized purposes.
- Implementing and managing authorized IS security programs.

- Working with the IS security staff to develop risk acceptance and management practices when security controls adversely affect operational effectiveness.

Second, the security responsibilities of IS owners involve:

- Determining the value of IS assets.
- Establishing levels of protection and control for IS assets based on their value and importance.
- Establishing access and use criteria for IS assets.
- Working with users, custodians, and the IS security staff to monitor compliance with the established levels of protection.

Third, IS custodians have responsibilities which include:

- Strict adherence to all owner-specified protection and control criteria for IS assets in their custody.
- Maintaining effective overall control to prevent damage or destruction that could adversely affect the owner's operational schedule.

4. The IS Security Staff

The IS security manager and his or her staff are the focal point for security activities within the organization. The staff also provides an advisory function to both top and line management. The IS security manager and staff must assume responsibility for several activities. In conjunction with top management, they must develop an organizational IS security policy and a structure for the assignment of security responsibilities for the overall organization and for each functional area. Also, they must establish operational standards and procedures for the implementation of the IS security programs by managers at all levels. Finally, they must develop and implement management systems and procedures for reviewing and evaluating organizational IS security programs, disclosing deficiencies, and recommending corrective actions.

D. IS SECURITY POLICY

1. Background

Once the decision to establish an IS security system has been made, a management commitment secured, and the IS security manager appointed, it is essential to establish an organizational IS security policy. The objectives and priorities of the system must be clearly defined at the beginning to achieve the desired level of system performance. There must be a clear understanding as to what is to be protected and why it is to be protected. [Ref. 27:pp. I-2-1 to I-2-3]

2. **Security Objectives**

The organizational IS security system objectives must be defined to establish a direction for the system. Such objectives were discussed in Chapter III, Section C. However, an organization may decide to modify such objectives to suit its own requirements. Once defined, the objectives should be set forth clearly and explicitly in a security policy statement. Such a statement should define the powers, rights, and accountabilities within the organization at the various levels to accomplish the objectives. Finally, the objectives statement should be widely distributed within the organization.

3. **Security Priorities**

The organization's security priorities should be delineated. Such priorities translate the general security objectives into more specific requirements that are based on the environment and the nature of the security tasks to be performed. There is a number of factors specific to the organization that will have a major bearing on the establishment of security priorities. Such factors include:

- *Organizational Functions.* A significant factor involved in setting protection priorities is the function or mission of the organization. In highly transaction sensitive organizations, such as financial institutions, the highest priority is established for protecting and monitoring critical transactions. Other organizations, such as manufacturing, may be highly process sensitive and the priority will be established so as to ensure the confidentiality of trade data processed. Service oriented organizations, such as consulting firms, will emphasize the protection of client data that would place them at a disadvantage should it become known to their competitors. Therefore, the security manager and staff must carefully assess the function of the organization when developing security priorities. [Ref. 27]
- *Availability of Security Resources.* The availability of IS security resources is another major determinant. Organizations with substantial resources committed to IS security will necessarily structure their approach differently than will an organization with more constrained resources. [Ref. 27]
- *Level of Dependency.* The organization's level of dependency can be a significant factor for establishing priorities. Priorities could concentrate more heavily on existing or anticipated resources and applications based on the organization's level at the time of security policy formulation.

E. SECURITY SYSTEM ENVIRONMENT ANALYSIS

1. **Purpose of the Analysis**

The purpose of this analysis of the security system's environment is to develop baseline security information and requirements. This will be accomplished by performing research surveys of the organization's environment, top management, and the IS. The information resulting from these surveys should be entered into a security database maintained by the security staff. The database will be a significant tool for the

development, maintenance, and operation of the security system by centralizing and securing the information needed to accomplish all three of these functions.

2. The Organization's Environment

The organization's environment should be surveyed to determine what security must be incorporated within the organization. The security measures result from environmental legal and regulatory strictures. The organization's legal staff, consultants, legal research, or professional publications could provide a means of obtaining relevant federal, state, local, and international laws that affect security system development. However, several significant laws will be briefly outlined as follows: [Ref.27:pp. II-1-2 to II-1-5]

- *Privacy Act of 1974 (5 USC 552a).* It established policy for collecting, maintaining, disclosing, and safeguarding personal information in federal systems of records.
- *Freedom of Information Act (5 USC 552).* It established policy for public disclosure of information, documents, and records maintained by the federal government.
- *Foreign Corrupt Practices Act of 1977 (FCPA).* This act changed the Securities and Exchange Act of 1934. It provided that all firms covered under the act (i.e., publicly held) must devise and maintain an adequate system of internal accounting controls.
- *Public Money, Property, or Records (18 USC 64).* This law established criminal penalties for embezzling, stealing, or knowingly converting to personal use or use of another any federal records or property.
- *Disclosure of Confidential Information (18 USC 1905).* This law established criminal penalties for disclosing trade information.

3. Organization's Top Management

The organization's top management should be surveyed to determine their IS security needs. This survey should extend beyond the members of the top management who are participating in the development of the security system. Surveys could be conducted using predetermined survey documents; group meetings; or individual discussions. Top management should be questioned concerning their opinions of the current state of security within the organization; any problems that they wish to discuss; their perspections of their security needs; and any suggestions that they may have as to the manner in which the security system should be developed, operated, and managed. Their security needs should be as narrowly defined as possible in terms of information and applications. This is especially important since top management generally uses specific kinds of information and applications to perform its responsibilities. For example, top management could be using a strategic planning application to support its planning responsibilities.

4. **The Organization's IS**

The conceptual framework of an IS, presented in Chapter III, Section B, should be used to perform an analysis of the IS. First, the IS should be surveyed by the members of the development group to determine its objectives and measures of performance. This information is important since such objectives and measures of performance could conflict with the established security policy. For example, to meet all users' requests for information, the IS may be providing information to users who should not be receiving it. Also, its measures of performance may not contain criteria for the reliability and protection of information and other assets.

Second, the IS's environment should be surveyed. IS users should be identified and defined. The identification of users involves determining their names; locations; work positions and responsibilities; their powers, rights, and accountabilities as users and the justifications for each; the extent of computer knowledge, skills, and experiences; and their history as users of the IS. Also, users are defined as consumers, owners, and/or custodians. A user can be defined as one of these, two of these, or all three of these types depending upon their rights, powers, and accountabilities. For example, a user could have the right to receive information; to own specified IS resources; and to act as a custodian for other IS resources. The identification and definition of users can be obtained by researching IS records.

The organization's line and staff tasks (e.g., accounting, marketing) and structures (e.g., departments, divisions) should be accounted for and users identified with each one. A survey of all or a sample of users should be performed to determine their security needs; problems; and suggestions. Such surveys could be conducted using predetermined survey questionnaires; group meetings; or individual discussions.

Third, IS resources (assets) should be identified. Appendix A provides a listing of defined IS assets. Each asset on the list is identified with a unique number. Appropriate information should be entered into the security database about each asset. Such information should include the names; locations; costs; performance history; operating status (e.g., under repair, fully operating); quantities; purpose of asset; producers; associated consumers, owners, and custodians; and identification data such as serial numbers, model number, and class number. IS and/or accounting department records should be examined to obtain this data.

Fourth, the component (tasks) of the IS should be surveyed to determine the extent of IS capabilities. The IS may not, for example, have a communications or

systems programming task. Systems programming may be performed under a contract with an outside vendor. On the other hand, the IS may not have a communications capability if it has a centralized configuration. The IS resources (assets) that are used to perform each relevant component (task) should be entered into the security database.

Fifth, the management of the IS should be examined. IS records could be researched and discussions held with IS management personnel to obtain some significant information. The configuration should be obtained to determine the extent of the structure and deployment of IS resources and components (tasks). IS plans should be reviewed to gain an understanding as to the planned direction of the IS. Existing applications and those under development or those expected to undergo development should be included in such information. This would provide some insight into determining the organization's level of dependency. Also, the information entered into the database should specify the technology and class of each application. All IS policy statements, standards, rules, procedures, and guidelines relevant to security should be obtained and read to determine the current level of management controls over its operations. Finally, a history of security violations, problems, and audit results should be accumulated and analyzed to determine trends and significant problem areas.

5. **Baseline Security Requirements and Information**

The surveys of the environment resulted in two significant accomplishments. First, information relevant to the development, operation, and management of the security system was obtained and entered into the security database. This information involved environmental laws and regulations which require the organization to secure specified assets; top management and user security needs; the IS objectives and measures of performance; user identification and definition; IS resources (assets); IS components (tasks); the IS configuration; IS plans and established security procedures; and the technology and class of each existing and planned IS application.

Second, the analysis resulted in the establishment of a baseline or minimum level of security requirements. These requirements resulted from the survey of environmental laws and regulations and the organization's internal security policy and existing procedures relevant to IS security.

F. SECURITY CLASSIFICATION PROGRAM

1. Background

It is not appropriate to approach the protection of automated systems and their associated data assets as a monolithic issue. [Ref. 27:p. I-E- 1] In other words, all IS applications, data, and transactions need to be afforded the same degree of protection. Such an approach to IS security would create several problems. First, all applications, data, and transactions do not possess the same level of sensitivity or criticalness. For example, an electronic funds transfer system that moves billions of dollars daily is, of course, far more sensitive than a capital asset accounting system. The same could be said of data. Data regarding an organization's strategic marketing plan requires a higher level of protection than does routine purchasing and accounting data. In order to determine effectively the level of protection required by its applications, data, and transactions, organizations must first identify the level of sensitivity and criticalness of those assets. Such an approach helps to avoid a situation of overprotecting some assets while underprotecting other ones.

A second problem that arises from a "shotgun" approach to security is that protection resources are frequently wasted, incurring unnecessary processing overhead and negatively affecting operational efficiency and productivity. For example, an unnecessary security software package excessively consume processing time that could be used for the processing of applications. Finally, an organization's inability to objectively identify and classify IS applications, data, and transactions according to their sensitivity and criticalness makes it difficult (if not impossible) to develop effective IS security standards. Without these standards, it is impossible to implement either an IS security system or an effective program of IS auditing.

Such problems can be solved by the development and implementation of an organization-wide IS Security Classification Program. Three benefits result from such a program. [Ref. 27:p. I-E-12] First, the classification of application systems and data on the basis of their sensitivity/criticalness permits controls to be allocated based on specific protection requirements. This results in a higher level of overall protection and reduced costs for security system operation. Second, the objective classification of applications, data, and transactions permits system development and maintenance personnel to readily identify sensitive and critical areas while implementing and maintaining controls during development or improvement. Finally, classification permits IS auditing to focus its activities on those applications whose sensitivity makes

them targets of fraud or whose criticalness makes their continuity of operations a matter of organizational survival.

2. **Establishing the Classification Program**

Implementation of the program should begin with the development of an organizational framework in which all IS applications, data, and online transactions can be analyzed, evaluated, and classified. [Ref. 27:pp. I-E-1 to I-E-2] One means to accomplish such a process would be the establishment of a Security Classification Review Committee. Such a committee would set policy and direct the efforts of several classification working groups. If this approach is used, the committee should be established at the direction of top management and should comprise the IS security manager, the IS auditor, and the manager of applications development.

Upon its formation, the committee should determine the order in which IS applications, data, and transactions will be reviewed. Due to the impracticalities of reviewing all such items initially, the committee should develop a list from the database of those items that it considers the most sensitive and/or critical. Generally, applications, data, and transactions should be reviewed in the following order:

- All online applications currently under development. Basically, it is less expensive and time consuming to apply controls to applications during their development than when they are installed and operational. Also, major disruption of IS service could result.
- Existing online application systems involved in money movement or management (e.g., electronic funds transfer systems, cash management systems).
- Existing online applications involved in the movement of nonmonetary negotiables (e.g., securities trading and movement systems).
- Existing online applications handling sensitive proprietary or personal data (e.g., strategic planning systems, client information systems, personnel systems).
- Online applications handling functions critical to organizational operations (e.g., ticketing/reservation systems, process control system).
- All new and existing batch systems.

Once the applications are identified and ranked in the order in which they will be reviewed, the committee must then manage the review process.

3. **Classification Evaluation Criteria**

The next step in the development of a classification program is to formulate criteria or variables for assessing the sensitivity and criticalness of the applications, data, and transactions. Such criteria will define sensitivity and criticalness levels in terms of the level of damage to the organization if specified IS assets are subject to destruction, modification, disclosure, or denial of service.

Since each organization has unique priorities relative to the sensitivity and/or criticalness levels of its applications and data, the Classification Review Committee should carefully evaluate the environmental analysis results previously discussed to determine the levels of protection required. Such an evaluation should be based on two basic properties of application systems, data, and transactions - sensitivity and criticalness.

a. Sensitivity

Sensitivity is the degree to which the organization will suffer damage of some tangible and/or intangible form if application systems or the data and transactions they store and process are subjected to one of the following: [Ref. 27:pp. I-E-2 to I-E-3]

- *Compromise.* Compromise may involve unauthorized disclosure of data (either accidentally or maliciously) or the theft of resources.
- *Modification.* Modification includes all types of modification, either accidental or malicious, that could result in fraud, damage to reputation, injury to competitive posture, embarrassment, or other negative impact on operations.

An analysis of applications, data, and transactions relative to their impact on overall operations if compromise or modification should take place needs to be performed by the review committee. A multilevel sensitivity classification matrix should result from this analysis. There are five parameters or variables which need to be considered when assessing sensitivity. [Ref. 36:pp. 2-4]

- *Competitive Value.* The actual or potential value that the data could have to other organizations. Such value can be quantified, such as in terms of potential dollar loss of business or service to customer or client, effect on market share, impact on net income, potential or unfavorable publicity, and so forth. The basic assumption is that the greater the value of data to a competitor, the higher the level of sensitivity. Therefore, the more stringent the controls that should govern its accessibility, usage, and disposition. Examples of data with such competitive value include data on the organization's current product (customer-satisfaction surveys, customer's master list, customer's list with products installed, marketing surveys, planned enhancements, list of distributors, design specifications, and cost figures), new product (design specifications, marketing surveys, competitive analysis reports, and potential customer list), and strategic planning (diversification plans, financial plans, planned acquisitions, and new product direction) [Ref. 33:pp. 6-7].
- *Fraud Potential.* This involves the extent to which the data could be used for personal monetary gain by those within or outside the organization. An example would involve any report indicating savings account activity that could be used to move money between accounts and reduce the risk of detection by operating within a time frame which is consistent with normal account activity. The basic measurement is the potential dollar loss to the organization if a fraud is perpetrated using the data being evaluated.
- *Legal Liability.* This involves the likelihood that the organization will be subject to legal action if the data is improperly disclosed. Also, legal liability could result during the normal course of business if data proves to be false or inaccurate (e.g., the 10-K or the annual report). This analysis variable could be expressed in terms of the cost of fines/litigation. Data of this nature involves such areas as personnel, health, credit, financial, account balance, salary, performance, and name and address data about individuals or organizations.

- *"Newsworthyness".* This is data which is or could be considered newsworthy by the media or special-interest groups. The underlying premise of this variable is that if the data is considered newsworthy by any of these organizations and is not made public through normal public relations channels, the data may be distorted or misinterpreted.

- *Financial Exposure.* Financial exposure involves the dollar value of the assets or liabilities of the organization. The commercial loan portfolio, for example, of a bank is a significant asset. On the other hand, commercial deposits are a significant liability. Since both of these financial items are volatile and represent a high value, they would place higher on the criticalness scale than data about fixed assets.

Although organizations have varying needs in terms of sensitivity levels, the classification process has many common factors. Appendix B presents a sensitivity matrix that can be expanded or abbreviated to meet specific requirements. It is offered as one means of structuring the sensitivity classification. However, an organization may develop whatever approach it regards as appropriate to perform the classification. The sensitivity levels (A-F), the numeric ratings (0-5), and the impact values (e.g., more than $10 million) could vary depending on the particular circumstances of the organization. For example, an organization's size may be so small that the impact scale should only have a maximum of $100,000 rather than more than $10 million. Each of the six sensitivity levels is assigned an equivalent numeric rating. For example, extremely critical and extremely sensitive are each assigned a numeric rating of 5 since they represent the highest levels of sensitivity and criticalness.

b. Criticalness

Serious loss can result to an organization if it sustains serious damage from denial or impairment of applications or data. Criticalness is a means of assessing the type of backup, recovery, and contingency procedures employed to ensure continuity of operations of critical components (tasks). There are six criteria or variables which need to be considered when assessing criticalness. [Ref. 37:pp. 2-4]

- *Cost of Creation.* This involves the cost in terms of time, manpower, facilities, services, and out-of-pocket expenses to create the resources and components. For example, research data (e.g., product or market research) is generally collected and recorded ("created") over an extended period of time. The significant or real value of the data may come from the conclusions drawn from it. Computer software represents a major example of the value of an IS resource which could exceed its recorded or development value.

- *Cost or Difficulty of Reconstruction.* This involves the effort which have to be expended and the cost which would have to be incurred if the resource or component had to be reconstructed following its destruction or loss of its integrity. Such is often the case with archival records. Both cost of creation and cost or difficulty of reconstruction should consider existing backup provisions. When these exist, cost evaluations must consider reprocessing, premium costs that could be incurred for additional resources to facilitate reprocessing, and costs of diverting existing resources from normal organizational activities.

- *Impact on Management Decisions.* This variable involves the extent to which management decisions could be affected if data becomes unavailable or its

integrity is violated. An example would be a problem with a bank's loan watch report. This report is used to identify potentially troublesome loans. If this report becomes unavailable, the number of bad loans might increase because lending officers would not have the information they need. Therefore, in this case, data can be viewed as impacting important decisions involving customer relations or activity.

- *Availability Constraints.* This variable involves the extent of the delay which can be tolerated between the time data is requested and the time when it is made available. For example, a 24-hour or more delay in providing a checking account customer with a list of all debits and credits against his or her account for the past 30-days should be reasonable. However, information about the bank's reserve position must be made available within a few hours after the close of the day's business.

- *Retention Constraints.* Such constraints involve the degree to which retention of the data is required by regulatory agencies and/or organizational management. An example would be certain segments of personnel data that must be retained for a period of time specified by the Internal Revenue Service (IRS), Equal Employment Opportunity Commission (EEOC) and other government agencies.

- *Processing Constraints.* This involves the degree to which the processing of the data is governed by organizational needs, management requirements, or regulatory demands; and the degree to which other resources and components depend on the availability and integrity of the data. Checks, for example, should be processed for clearing within 24 hours; customer funds must be transferred within the agreed-on time frame; the bank's reserve position must be determined at the close of each business day. In each case, the data needed to perform the required functions has processing constraints.

Using such criteria, criticalness classification levels could be developed for analyzing applications, data, and transactions. Appendix C presents a criticalness matrix that can be expanded or abbreviated to meet specific requirements. As with Appendix B, each of the levels is assigned a numeric rating to represent its relative significance within the level (e.g., 5 is a higher level than 4). Also, this matrix is offered as one means of structuring the criticalness classification. It is rare for sensitivity and criticalness levels to coincide. A specific transaction may be extremely critical to overall operations but may present no potential for fraud or other misuse. Therefore, a classification scheme should be developed for each of these properties, with the continuity of operations of applications being given the same consideration as protection against modification or compromise.

At this time, it is important to stress caution when using Appendices B, C, and G. These three were constructed using an ordinal measurement scale. As indicated in the appendices, this scale only represents position in an ordered series. It does not represent the magnitude of the difference which exists between the successive positions in the scale. In other words, sensitivity level A with a numeric rating of 5 indicates that it is of greater significance than E with a numeric rating of 1. However, it is not necessarily five times as great. In fact, $10 million with a numeric rating of 5 is a thousand times greater than $10,000 with a numeric rating of 1.

On the other hand, a numerical assignment of a ratio scale reflects identity, order, and differences in magnitude. An example of such a scale would involve measuring height by a yardstick. A person with a height of six feet is twice as tall as someone who has a height of three feet. In the case of the three appendices, this would mean, for example, that sensitivity and criticalness level A would be five times as great as level E. [Ref. 38:pp. 62-64]

The use of the ordinal scale will prove useful for several reasons. First, it is difficult to establish precise dollar limits for the various levels of sensitivity and criticalness. Extremely sensitive, for example, is greater than highly sensitive but no defined criteria exists to establish precisely by how much of a difference does exist. The determination of the difference becomes a matter of professional judgement and historical experience. Second, the dollar range of the scale will vary depending upon the size of the organization. A large organization may have a dollar scale as large or larger than the one presented in the appendices. For example, a small organization may have the range $100,000 to $1,000,000 as the top level of the scale. On the other hand, a larger organization, may have a top level of more than $100 million. Third, it must be emphasized that a numeric rating of 5 does not necessarily mean that an application program, for example, would require five times as many controls and attention as an application with a rating of 1. The rating is a guideline that should be used in conjunction with other factors during practical design to apply a sufficient level of protection to assets. The various classification levels also provide a means of classifying known controls by those levels where they can be most effectively applied.

c. Classification Program Implementation

Upon the establishment of the levels of sensitivity and criticalness, the Classification Review Committee must set policies and guidelines concerning implementation of the program. The committee must consider two key areas in doing this. First, there is the issue of classification authority. Authority for assigning sensitivity and criticalness ratings should reside with the user of the application or data. It is the user who will ultimately feel the impact of the compromise or modification of data or the denial of service. Therefore, ownership of all applications and appropriate data must be clearly assigned to user organizations, which then assume complete responsibility for determining the classification levels of their respective applications, data, and transactions. However, the results of user classifications should be reviewed by the committee. This is necessary to prevent under- or over-classification of assets.

Operational managers using IS resources should be formally delegated (in writing) by top management through the Classification Review Committee, the tasks of reviewing applications, data, and transactions in their task areas and of assigning classification levels to these resources. Responsibility for this review should be placed at a high enough level within the user community (e.g., vice president, manager) to ensure that it receives adequate management attention.

Second, once classification authority has been assigned, the appropriate managers must be required to submit a schedule of classification review and evaluation action to the review committee. The committee then needs to actively monitor review and classification activities within the various task areas. Timely action can be ensured if the internal audit function also monitors progress as part of its regular controls review.

In addition to its oversight responsibilities, the committee should establish procedures to ensure that all new resources are reviewed and classified during acquisition or early in their development life cycle. Also, provisions should be made to reevaluate resources periodically (e.g., every two years) to ensure that assigned sensitivity and criticalness are still adequate and appropriate.

4. **Classification Review Process**

Individual classification working groups should perform the actual review and analysis of the sensitivity and criticalness of application systems, data, and transactions. [Ref. 27:pp. I-E-5 to I-E-12] Such groups, appointed by those managers having classification power and responsibility for applications and data, should comprise representatives from IS security; IS auditing, applications systems project management, and user management. The level of sensitivity and criticalness should be recommended by the working group to the responsible manager, who makes the final decision concerning classification.

a. Data/File Classification Review

The first step in this process is to perform the Data/File Classification Review. The working group should identify each file used by the applications and analyze it using Appendices B and C. This analysis of sensitivity and criticalness is based on several factors. First, the organization's history may prove a valuable source of information for estimating the various classification levels. For example, the disclosure of competitive data could have resulted in loss of business or the gain of business for another firm. Second, various laws may specify the classification levels of

various data such as personal or health data. Third, the professional judgment of the working groups could play a significant role in deciding on the classification levels. The results of the review should be entered into the security database. The information to be entered includes the name and/or alphanumeric file designator; applications using the file should be identified and a functional description of the file's data. Each member of the working group should then independently assess the sensitivity and criticalness of each file using the criteria of Appendices B and C. The members of the working group should jointly examine their findings and agree on the rating to be given the file in each of the four sensitivity/criticalness areas. Using the numeric ratings assigned in these categories, the group should then assign an overall sensitivity/criticalness level for the file based on the matrix presented in Appendix D. As the appendix indicates, extremely sensitive (A) and extremely critical (G) are assigned the same numeric rating of 5. It is rare for the two to coincide. For example, a specific transaction may be extremely critical to overall operations (5) but may present no potential for fraud or other misuse (0). The ratings are assigned to provide some means of assessing the relative significance for the varying levels of sensitivity and criticalness. The sensitivity level is determined by the highest of the three sensitivity ratings. For example, if the competitive data level is A (5), the data with fraud potential is E (1), and the privacy data is at F (0), then the overall sensitivity is rated at the highest of the three which is A (5). The overall sensitivity/criticalness level should then be entered in the database for that specific file.

b. Transaction Classification Review

If the application system being evaluated is an online application, the next step is to perform a Transaction Classification Review. While the data/file classification review defines sensitivity and criticalness at the database or file/data set level, sensitivity and criticalness for online applications must also be defined at the transaction level. Therefore, the group must identify each online transaction and its sensitivity and/or criticalness level. There are two approaches for transaction classification.

The first approach involves having the application development manager identify all files accessed by the transaction. This information should then be entered into the security database. The sensitivity and criticalness levels of the online transaction should be determined in the same manner as the data/file review previously discussed.

The second approach is to classify transactions by generic type and assign a ranking to each based on their scope and function. The following are the basic types of transactions, ranked in order from the most critical to the one requiring the least protection. [Ref. 39:p. 69]

- *Type 1.* These transactions affect the total IS operation. There exists the potential that damage or a complete shut down could affect the entire IS operation.
- *Type 2.* These are transactions that directly relate to the IS security system itself. There is the potential that a transaction would render security software inoperative.
- *Type 3.* These transactions are not bound to any specific applications. Examples involve debuggers and software tools that enhance programming productivity. There exists the potential that a debugger, for example, could be used to access security files and gain access to passwords and user identification codes.
- *Type 4.* These are the so-called "back-door" transactions which are designed into the third-party software. A back door is a simple transaction that a programmer designs into his or her program so that he or she can get into the application file quickly for debugging and maintenance. Since only the programmer is aware of this transaction, and it isn't published in the documentation, users have no way of learning it.
- *Type 5.* These transactions within an application program that are used to update application files.
- *Type 6.* These are inquiry transactions which are not bound to a specific application.
- *Type 7.* These are inquiry transactions which are specific to a given application.
- *Type 8.* These are transactions with no security associated with them.

c. Applications Review

The third step in the review process is the analysis of the overall level of sensitivity and criticalness of the application. In this phase, the working group identifies the application and provides a brief functional description of overall application operation. All files and transactions identified and analyzed during the previous two processes and their associated sensitivity and criticalness data are then entered into the security database. This presents the working group with a profile of the application, including its data and transactions, as well as an objective basis for determining application classification in terms of sensitivity and criticalness.

In developing overall application ratings, the working group should analyze the sensitivity and criticalness levels of all files and transactions within the application. The ratings assigned to the application should reflect the highest level assigned to any of the constituent parts (e.g., a rating of Extremely Sensitive for any file or transaction would render the entire application Extremely Sensitive). This ensures that the level of

security and management review afforded the application will be sufficient to protect the integrity of all its data and transactional parts.

G. CONCLUSIONS

The planning process resulted in the accomplishment of several significant results. First, a development group was established to perform the planning, design, and implementation of the security system. Security system development plans were formulated with estimates for staff, funding, and time requirements. Second, the security responsibilities of top, line, and security managements were established. Third, an IS security policy was formulated. This policy established both security objectives and priorities. Fourth, the laws and regulations which impose mandatory security requirements on the organization were identified along with any relevant organizational IS security policies and procedures. Fifth, top management and user security needs and concerns were identified. Sixth, IS assets and users were defined and identified. Finally, a Security Classification Program was established. IS applications, data, and transactions were identified and assesed as to their sensitivity and criticalness. The accumulated information was entered into the security database. The information will be used as input to the design process which will be subsequently discussed.

V. THE DESIGN PHASE

It's on the path you do not fear that the wild beast catches you. [An African Proverb]

A. INTRODUCTION

The design phase involves a process which results in the establishment of the security resources (controls) part of the IS security system. Such controls are applied to the resources (assets) of the IS to provide the required level of protection for the assets. This application of security controls to IS assets results in the linkage or connection between the IS security system and the IS. This linkage is produced by a process consisting of five activities. First, threats to assets will be identified. Second, an assessment will be conducted of the impact of such threats upon the assets. This will involve assigning values to each asset including the logical assets (software and data). Third, a determination as to the current security posture of the IS needs to be performed. This will result from the information accumulated in the security database during the planning phase as well as a security survey. The current security posture will be compared with the results of the threat assessment to determine whether the current level of protection is adequate to counter identified threats. If the current level is not adequate, then a state of vulnerability exists. Fourth, a logical design should be performed. This design represents a "virtual" design since all identified assets and threats are matched with all possible controls needed to counter such threats. Also, it represents the maximum possible protection that an organization could develop. Fifth, a practical design should be developed based on the utilization of specified criteria and constraints to the logical design. This practical design will result in a control configuration consisting of assets, threats, and selected controls.

B. A RISK ASSESSMENT

1. Background

The activity of a risk assessment involves a detailed examination of the assets and procedures of the IS; the vulnerabilities of the existing controls; and the threats that may exploit such controls and result in the disclosure, modification, destruction/damage, and denial of service of assets; and a determination of the current

security posture of the organization. [Ref. 40:p. E-1] The purpose of the assessment is to help top management, IS management, and security management strike an economic balance between the impact of risks and the cost of protective controls. A secondary benefit is the increased security awareness which will be apparent at all organizational levels. [Ref. 41:p. 3E-2] There are three tasks needed to accomplish the risk assessment. First, threats which are existing and potential to assets will need to be identified. Second, the economic impact of such threats will need to be estimated. Third, a survey of existing security controls which are applied to counter those threats will need to be conducted. A subsequent assessment will be made to determine the extent of the vulnerability of the assets to those threats.

2. **Threat Identification**

The first task of the risk assessment activity is to perform a threat identification. During the planning process, IS applications and their associated data and transactions were classified. The purpose of the classification was to determine the relative criticalness and sensitivity of the applications, data, and transactions. In effect, all applications, data, and transactions were prioritized based on defined criteria. The prioritization will play a significant role during the actual allocation of security controls within the IS as will be demonstrated during practical design.

Threat identification will involve an identification of threats to the assets which are used to form such applications, data, and transactions. As discussed in Chapter III, applications are what IS management develop to accomplish its objectives. Facilities, hardware, software, data, people, and procedures are combined and allocated to form the applications.

A threat to an IS asset is any circumstance or set of circumstances that possesses the potential to cause harm. [Ref. 27:p. II-2-1] There are several means to perform an identification of threats. First, the security database should be accessed to provide a source of threats. The database contains the history of security violations and problems which were recorded during the planning phase. This information should involve the causes and frequency of violations and problems. Also, the nature and locations of assets and components (tasks) can provide insight into threats. For example, IS assets may be located in geographic areas which are suspectible to flooding and snowstorms. Also, the IS may contain a communications component (task). Therefore, there is the threat of the failure of communications software. Second, professional publications from such organizations as the Computer Security Institute

could provide information regarding possible threats for specific assets. Third, professional consultants specialize in performing risk assessments and could provide information on various threats.

Appendix E contains a listing of threats and some examples. [Ref. 27:pp. II-2-1 to II-2-17] The threats are categorized as to their primary cause or source. Natural occurrences, such as floods and fires, pose a threat to all assets. Human intervention cannot eliminate these threats. Prior planning or controls implemented cannot prevent their occurrence completely. However, by acknowledging the presence of a threat, the organization can take steps to minimize its damage. Another source of threats involves the technical operation of supporting utilities, hardware, and software. Such threats may result from problems beyond the control of the organization (e.g., failure of the supporting electrical utility or the communications common carriers) or from negligence on the part of organizational personnel (e.g., improper maintenance of heating, ventilating, and air conditioning equipment, failure to follow established procedures for operation of hardware). Next, human accidental threats represent the most common threats to IS operations. These involve errors or omissions on the part of the personnel of the organization. The final category of threat presented in Appendix E represents hostile acts of malicious intent on the part of persons within or outside the organization. An inventory of threats and estimates as to their probabilities should be maintained and updated in the security database. Appendix F is an matrix which matches each asset with the events that pose a threat to it. This matching of asset to threat is one that has developed from historical experience as well as from professional testing and research.

3. **Impact Analysis**

The purpose of an impact analysis is to assess the damage which could result from an unfavorable event (threat) and an estimate of how often such an event may happen. The damage can be expressed as the destruction, modification, denial of service, and disclosure of assets. These forms of damage can be measured in both monetary and nonmonetary terms. However, the nonmonetary impact should be converted to an approximate monetary impact. This will permit sufficient comparisons between alternative security controls. There are four steps needed to perform the impact analysis. An explanation will be made of each of the four steps.

a. Step One

The first step in the analysis is to determine how broadly or narrowly to define the assets contained within the security database (Appendix A). For each defined asset, all units of this asset should be in the same physical area, protected in the same manner, and subject to damage by the same threats. If one unit of the asset is damaged, either all other units must be highly likely to be damaged in a similar way, or the entire asset should be rendered unusable. For example, six identical computers are to be considered as six separate assets because damage to one of them would not imply damage to all of them. On the other hand, do not regard a single computer as a collection of subparts, since if one of these components were to fail, the entire computer would be damaged to a similar level. Also, it may not be practical to break data assets down to individual files (tapes, disc packs, etc.) for the purpose of assigning an impact value. [Ref. 40:p. E-4]

b. Step Two

The second step of the analysis is to determine which impacts would affect the designated assets. The following definitions of impact areas should be used: [Ref. 40:pp. E-4 to E-6]

- ***Modification.*** The value of logical (software and data) assets should be based on the cost to correct the consequences of the modification and/or the cost of locating and recovering from the modification itself. The value of physical and human assets (facilities, hardware, and people) should be based on the total cost to detect, locate, and correct the modification.

- ***Destruction.*** Destruction results in the loss of the asset. The value of the asset should include the cost to reconstruct or replace the asset, as well as the costs incurred from denial of service caused by the destruction. The impact values of software or data assets should be based on the cost to replace the asset. This value should include the cost of reconstructing the asset from scratch or the cost of importing and updating a copy of the asset. Labor costs required for this reconstruction should be included. As many factors as possible should be considered in determining the value. For example, if reliable backup tapes are readily available, the impact of destruction of a data or software asset may be negligible. Hardware and procedural asset impact values should be based on replacement or reconstruction of the asset. Generally, this would include the purchase or construction price of the replacement. However, in some cases, relocation costs might be considered.

- ***Disclosure.*** All financial, proprietary, and personal data should be assigned an impact value for the impact of disclosure.

- ***Denial of Service.*** This estimated value should include the costs incurred from all denial of service, except for that caused by the destruction of the asset. For example, a power outage to hardware may result in denial of service to users without actually destroying the hardware. The impact values should be based, when possible, on additional costs incurred and penalties assessed due to delays in job completion. Also, an impact value should be assigned for denial of service if operations should be delayed or cancelled or if appreciable delays result. The quantification of such intangibles should be based on a typical case and consider the extent of the denial and the importance of the operation or decision. A denial of service value should be assigned to key personnel if their absence would result in delays similar to those outlined above.

c. Step Three

This step involves estimates as to the monetary and nonmonetary impacts for each of the four impact areas just discussed. If the impact area affects the asset contained in the database inventory, then the economic loss which would result from the impact should be estimated. This loss can be measured in both monetary and nonmonetary terms. However, the nonmonetary impact should be converted to an approximate monetary impact to permit sufficient comparison between alternative security controls.

The National Bureau of Standards (NBS) [Ref. 41:pp. 3E-6 to 3E-8] indicates that the time needed for the analysis will be considerably reduced, and its usefulness will not be decreased, if both monetary and nonmonetary impact and frequency estimates are rounded to the factor of ten indicated in Appendix G. There will be no significant difference in the overall exposure whether the damage from a specific threat is estimated at $110,000 or $145,000. Also, assigning value to such things as loss of career caused by disclosure of confidential information or suffering caused by undue delay in the delivery of an annuity check is, in fact, more readily performed in orders of magnitude (1, 2, 3, etc.) than in actual figures.

The sources for impact estimates include the organization's historical accounts of security violations and problems; suppliers of the various assets; and professional consultants. Using the estimated monetary impact amount, refer to Appendix G and select the corresponding impact value rating (1, 2, 3, 4, 5, 6, 7, and 8) and enter this data into the database for each asset when appropriate. In other words, for a given asset, an impact rating of from one to eight should be assigned to each of the four impact areas of modification, destruction, disclosure, and denial of service. If the impact does not affect the asset, then no entry is made for that asset in the database. For example, disclosure of privacy data has a definite impact. However, disclosure of the software program that processes that data may not have an impact. Sufficient information which supports the impact value rating assigned should also be entered into the database. [Ref. 40:pp. E-1 to E-9]

d. Step Four

The final step involves the computation of the annual loss expectancy (ALE). If the impact of the threat, i.e., the precise damage it could produce, and the frequency of occurrence of that threat, i.e., the exact number of times it could happen, could be specified, the product of the two would be a statement of loss. However, since

the exact impact and frequency can usually not be specified, it is only possible to approximate the loss with an ALE. This represents the product of the estimated impact dollars (I) and the estimated frequency of occurrence per year (F). For ease in use, the orders of magnitude for estimated frequency of occurrence can be indexed as shown in Appendix G.

The National Bureau of Standards (NBS) has developed the matrix presented in Appendix H. It could be used to compute the ALE of each asset for each of the four impact areas. The impact value and the frequency of that impact will be estimated for the appropriate asset/threat combinations which are recorded in the database. This will be accomplished by matching the estimated impact (i) and frequency (f) values for each threat that is associated with a given asset. The intersection of these two values in Appendix H results in the ALE. Therefore, for each threat that is associated with a given asset, there could be ALE values for the four possible impact areas of disclosure, destruction, modification, and denial of service. The four step process just described assumes that threats are mutually exclusive and does not account for their intersection. The results of the impact analysis should be recorded in the database.

The information which results from the impact analysis and recorded in the database could be summarized in several ways. First, for each individual asset/threat/impact area combination, there are estimated impact, frequency, and ALE values. Second, the total ALE for each asset within an impact area (destruction, modification, denial of service, and disclosure) can be derived. In other words, the ALE for all database management systems (DBMS) that are subject to destruction can be described. Third, the total ALE by individual threats within an impact area can be obtained. In other words, the ALE for the unauthorized modification of application software can be obtained. One example would involve the total ALE for the threat of unauthorized modification of application software. Fourth, the total ALE for each impact area can be determined. For example, the total ALE for the disclosure impact area can be obtained. Finally, the total ALE for all four of the impact areas can be determined. This would represent the total estimated loss that the organization would face from the four combined impact areas of modification, destruction, disclosure, and denial of service. It is important to stress that each of these estimated values will change as revised estimates are made of impact (i) and frequency (f) variables.

e. Vulnerability Assessment

The final step in the risk assessment is the performance of a vulnerability assessment. This assessment involves three items. First, an asset subject to loss. Second, a threat(s) to that asset that could result in damage to it. Third, the state of security, in terms of the lack of or weak controls, that would allow the threat to cause damage. Asset and threat information are already recorded in the database. A survey of the security controls which have been applied to IS assets will need to be performed.

Appendix I provides a listing of security controls which can be applied to assets to provide protection from various threats. Each listed control is assigned an identifying number. A survey should be performed to determine which of these controls, if any, are currently applied to IS assets. IS records should be reviewed and personal inspections made to determine the extent of the controls applied to assets. If the controls applied against assets to counter threats are insufficient to adequately protect the assets then vulnerability exists. [Ref. 35:p. 166]

The degree of adequacy of existing controls can be determined in several ways. First, the database should contain whatever information is available regarding the history of security violations and problems of the IS. The historical performance of the controls can be reviewed to estimate the degree of adequacy of the control in countering specified threats. The historical records may reveal vulnerability. Second, if history is not available or is immaterial in volume, then control reliability information could be obtained from outside sources. Such sources could include professional publications and vendor material. Third, tests could be performed to estimate the reliability of existing controls against a variety of threats. The threat conditions applicable to the asset could be simulated and the reliability of the controls applied to those assets estimated. Examples would involve both physical and logical access attempts; the inputting of erroneous data; and power failures. The results of the vulnerability assessment should be recorded in the security database. The discovered vulnerabilities should be ranked based on which provide the greatest, great, and least threats to the previously classified applications, data, and transactions. For example, does vulnerability 1 pose the greatest, great, least or no threat to all applications, data, and on-line transactions which were classified as extremely sensitive and critical, and so on? This threat to the various applications, data, and transactions should be expressed in economic terms as was previously discussed. The results of the vulnerability assessment should be recorded in the security database.

C. LOGICAL DESIGN

Logical design involves the expansion of the currently existing inventory of controls contained in the database to include all possible controls which could be used to counter identified threats. This expansion leads to the development of what may be called a "virtual" design since all identified assets and threats are matched against all possible controls needed to adequately counter such threats and protect the assets. Other things being equal, logical design represents the maximum possible protection that could be applied without regard for such factors as funding limits and the adequacy of the current level of protection. This design represents an inventory of appropriately matched controls. Appendix J provides a matrix which consists of controls which are identified with specific threats and assets. It matched each asset/threat combination which was identified in Appendix F with corresponding controls. This information should be entered into the security database.

Controls can be identified from several sources. First, the organization may have existing controls and historical records of their performance and suppliers. Second, there are organizations that provide such controls such as vendors who produce and market security software packages and fire detection devices. These vendors provide demonstrations of their products and offer material describing their characteristics. Third, professional publications provide information on existing and newly developed security controls. Fourth, vendors offer public fairs of their products at different locations throughout the country.

As much information as possible should be recorded about the controls in the database. Such information would include the control name; purpose; series/model/class/type/line; vendor; cost; ease of use; reliability; development and installation time; state of the art status; availability; insurance requirements; skill level needed to develop, install, and operate; and possible impacts on IS performance and availability if employed. The logical design will be used to support the practical design which follows.

D. PRACTICAL DESIGN

The practical design involves the construction of a configuration of assets, threats, and controls which will be applied to the threats to protect the assets within specified constraints. The logical design matched each asset and threat combination with a number of controls which could be used to counter the threats. However, due to

several reasons, all the controls cannot or should not be applied to the assets to counter the threats.

First, the practical design is subject to funding constraints which were imposed by top management during the planning phase. Second, specific IS applications, data, and transactions were previously classified as to their sensitivity and criticalness during the planning phase. Each application and its associated data and transactions were assigned levels of criticalness (extremely critical, highly critical, critical, moderately critical, minimumally critical, and noncritical) and sensitivity (extremely sensitive, highly sensitive, sensitive, moderately sensitive, minimumally sensitive, and nonsensitive). Therefore, applications, data, and transactions can be prioritized based on their criticalness and sensitivity. One application, for example, could have a higher priority than another application. The higher prioritized application would justify more protection over one that is less in priority. Third, the previously performed vulnerability assessment could have revealed that the surveyed classified assets were in various states of protection due to the strengths of the existing applied controls. Therefore, some of the prioritized assets will require the additional application of controls and some assets will not. Fourth, the controls which are recorded in the database can be further divided as to their applicabilities by sensitivity/criticalness levels. In other words, some controls are more effective against extremely critical applications and some are not.

The personnel responsible for the practical design must select the most cost-effective controls from among those listed in Appendix K. The appendix is a breakdown of the total number of controls listed in Appendix I. It applies each of the controls to specific sensitivity and criticalness levels. This matching of control to classification is one that results from historical experience and testing of the controls to determine their capabilities and reliabilities. For example, control number 34.1 involves the locking of all data and program files in a fire-resistant room or container when not actually in use. The access to the files should be limited to authorized personnel only. This control has proven to be applicable to all six levels of criticalness. The cost of each control as recorded in the database should be considered in three different ways: first, in regards to the ALE reduction that it brings about, then the total cost of the combined controls should be considered in relation to the net ALE reduction, and finally the additional ALE reduction by each control should be compared to its share of the total cost. For a control to result in a monetary savings, the amount saved over

the life cycle of the control must exceed the cost of its installation and maintenance. Any control which meets this specification is considered cost-effective. [Ref. 40:p. E-10]

THREATS	ITEMS	A	B	C	D
1	(a)	$20,000	$20,000	$18,000	
1	(b)	9,000	15,000	8,000	
1	(c)	11,000	5,000	10,000	
2	(a)	10,000	12,000		
2	(b)				
2	(c)	10,000	12,000		
3	(a)	4,000	6,000		
3	(b)	1,000			
3	(c)	3,000	6,000		
4	(a)	2,000	4,000		
4	(b)	5,000	2,000		
4	(c)	-3,000	2,000		

Source: Ref. 41:p. 3E-19.

Figure 5.1 Array of Controls vs Threats.

By constructing a matrix such as shown in Figure 5.1, the threats and the controls which could affect one or more of them can be displayed. The threats should be arranged in order of the ALE attributable to them (highest to lowest). Each intersection in the matrix should contain three items of information: (a) the estimated ALE reduction, (b) the annual cost of the measure, and (c) the resultant annual saving. Great precision is not required in obtaining these figures. The annual cost of a measure is presented opposite the most serious threat which it affects; opposite any other threat which is affected only the increase in cost to cover that threat is noted.

The cost-effectiveness of the previously identified existing controls should be evaluated as well. The existing controls should all be included in the matrix but only the annual maintenance costs need be considered, not the initial installation costs since those have already been expended. The cost of controls which are not used solely for the purpose of IS security should be prorated if possible. It is also the proper time to consider replacement costs. The replacement of equipment should be treated like any other remedial measure. The situation could arise that the cost of replacing equipment is less, in some cases, than its protection.

Comparing all the controls which remedy the same threat (or lesser included threats) will indicate which one is the most cost effective in the given circumstances. In Figure 5.1, control A, costing $10,000, provides a $24,000 saving against threats 1, 2, and 3 while control B, costing $17,000, provides a $25,000 summed saving against threats 1, 2, 3 and 4. The two controls combined, at a cost of $27,000, provide an ALE reduction of $49,000. However, the final comparison indicates that the $10,000 expenditure for control A only produces an additional saving of $6,000 over that obtained by the $17,000 expenditure. In some cases, it may be determined that the additional reduction is necessary; in other less sensitive situations, the cost saving will be adopted instead. In addition, care should be exercised to insure that the controls chosen to counter certain threats do not increase the estimated frequency of other threats.

With all of the ALE reduction and cost estimates arrayed, various combinations of controls can be considered tentatively until a satisfactory aggregation of security controls is achieved. The matrix will prove useful in explaining to top management why particular controls should be selected for testing and installation. [Ref. 41:pp. 3E-18 to 3E-19]

E. CONCLUSIONS

The design phase results in the selection of a configuration of assets, threats, and controls. The selected controls represent the establishment of the security controls part of the IS security system. The following chapter will involve sufficiently implementing the selected controls. This implementation will establish the link between the two systems.

VI. THE IMPLEMENTATION PHASE

To err is human; to really foul up requires a computer. [Bill Vaughan]

The psychic task which a person can and must do for himself is not to feel secure but to be able to tolerate insecurity. [Erich Fromm]

A. INTRODUCTION

The operations phase will involve a process of security system installation, testing, and management. First, the selected controls that have been approved will need to be implemented during a period of installation. Such installation should be performed in an orderly planned manner with accompanying user and security staff awareness and training. Second, the controls which resulted from the design phase process will need to be tested. This testing is required to ensure that the entire control configuration as well as its individual control elements are functioning as required. Such testing should be performed on a continuous basis as new controls are added to the configuration over time. Finally, the management and components (tasks) parts of the security system will need to be established. These two parts will permit the proper operation and management of the security system.

B. INSTALLATION OF CONTROLS

After the selection of controls, the security staff must concentrate their efforts toward the installation of the selected controls within the IS. Like all projects, the security system development must compete with other organizational programs for recognition and resources. To ensure the greatest probability of success, the security manager should make the following preparations.

First, the security manager should develop a prioritized list of requirements that need top management approval and/or funding. Such requirements should be based on the practical design analysis which was performed during the design phase. They should also reflect other organizational considerations, such as current cash position or market pressures, that might not have been fully reviewed in the analysis. Finally, it is important that the list should address not only the acquisition of security resources and services but the top management decisions that must be made to initiate or facilitate program implementation.

Second, it should be specifically indicated what is necessary for implementing the proposed program. The significant part of this process is the development of a realistic estimate of financial, personnel, and other resources needed to implement a given recommendation. These estimates were developed during the planning and design phases. However, circumstances may require revised estimates.

Third, detailed technical specifications covering IS security controls that must be developed or procured should be produced. Such development and procurement should be performed in conjunction with technical personnel. Fourth, a comprehensive acceptance test plan should be developed in conjunction with the technical and management staffs.

C. TESTING AND EVALUATION OF CONTROLS

1. Test Planning

The development of a test plan which defines the scope of the test must be considered first. The assumptions regarding how the system is supposed to operate; the effectiveness of security features; the reliability of personnel; and the actions of the user are to be challenged. The testing process should provide for the analysis of these areas. There may be some areas which do not require explicit testing. However, the practices and procedures used should be analyzed to ascertain the adequacy of protection and to identify potential problems. The testing process should encompass a detailed examination and attempted systematic subversion (singly and in combination) of the security controls and features of the system. It is understood that operating procedures will vary widely among different organizations. However, certain basic areas should be included in any test plan. [Ref. 27:pp. III-1-1 to III-1-2]

- *Physical Security.* The major concern in this area is determining whether there are exploitable gaps in the physical security of the system, including the central computer facility and remote terminal areas. The security of the physical plant ; heating, ventilating, and air conditioning systems; power distribution; fire detection and suppression systems, and so on should be tested and evaluated. Special attention should be paid to areas where the degrees of control and protection are not consistent and locations where resources are geographically removed from the central facility.

- *Personnel Security.* Tests in this area should determine whether all personnel with access to IS resources have been properly screened and have received security training. Also, the testing should review the adequacy of security training and of programs designed to ensure the loyalty and reliability of IS personnel.

- *Hardware and Software Security.* The emphasis with this area should be on testing the security features of the hardware and software separately and in combination, and on determining the ability of these features to prevent malicious exploitation of IS vulnerabilities. The plan of the test should involve hardware, systems software, and application programs to ensure that the execution matches the documented specifications and that system integrity is maintained.

- *Communications Security.* All communications hardware, software, circuitry, and installation procedures should be examined and tested to ensure that an adequate level of protection is maintained throughout the communications system. Specifically, this involves checking the security of front-end processors and/or communications controllers, hard-wired communications links, and the interface between the computer and the network as well as the proper functioning of cryptographic systems.

- *Procedural Security.* The purpose of testing in this area should be to identify deficiencies in operational procedures and/or their execution that could be exploited for unauthorized disclosure or modification of data or the denial of service. Also, it should be determined whether appropriate handling procedures and administrative controls are being enforced for the level of information being processed or stored in the system. Testing in this area may overlap, to some degree, testing in other areas due to the integrated nature of most systems. Areas that should be covered include procedural implementation of organizational security plans; computer center operations; terminal operation procedures; system software and application program development procedures; and emergency procedures.

2. The Test Team

At the conclusion of test planning, the security manager should organize the test team. It is not likely that the security manager and the staff will possess all the necessary personnel, technical skills, and, therefore, other personnel should be made available to provide assistance. Guard force workers, for example, can be invaluable in evaluating physical access control, their own operations, and overall security of physical resources.

Personnel or human resources department workers can aid in testing and evaluation preemployment screening, security training, and terminal practices. Communications personnel can test cryptographic systems, communication hardware, and communications facilities. Members of the programming/computer operations staff members can assist in developing and conducting technical tests of hardware and system and application software. Such personnel can also assist in evaluating technical test results and in formulating enhancements based on this testing. [Ref. 27:pp. III-1-2 to III-1-3]

3. The Testing Process

It is important that a detailed schedule and procedures for the actual testing should be developed. The tests should be conducted so as to cause as little disruptions of normal operations as possible. Generally, testing should not be performed when the system is utilized for software development or testing; during implementation of new hardware or software; or during critical processing cycles such as payroll or billing.

a. Testing Tools

There are a number of tools which could be used to perform the tests. Such tools can be specifically applied to each control. For example, a significant security

hardware device is an emergency power system. Tests of such a system should include a review of its inspection records to determine if inspections are being performed as required; and to conduct periodic tests through simulations of power outage conditions. The security database should be further expanded to include an inventory of appropriate tests for each control in the database. There may be multiple tests, as indicated, for each control. Therefore, each test should be specifically designated to distinguish it from other tests that could be applied to that control. [Ref. 27:p. III-C-2]

b. Conducting the Tests

There should be comprehensive recording of the testing process in the security database. The control tested; the testing tool(s) used to perform the tests; the test dates; and the results of the tests should be recorded. A standard test report should be designed to be used to report the results of all tests. [Ref. 27:p. III-1-3]

4. **Test Evaluations**

The evaluation of test results should only be performed after all testing is complete. Some tests may review a control for more than one protective quality or may require several steps. For example, a security guard force provides protection against unauthorized physical access. Also, it provides a means of visually detecting fire, internal flooding, and the like. Therefore, testing the performance of the force involves testing its training and procedures in all areas.

In those areas suffering minor deficiencies, the security manager should review the deficiencies with the manager responsible for that area and attempt an on-the-spot correction. If the deficiency is corrected, no additional action is required. On the other hand, if deficiencies are extensive or particularly severe, or when corrective actions will require a substantial outlay of resources, then the results of the team will require review and evaluation by top management.

a. Recommending Security Enhancements

After the performances of tests and their recording on the database, the team should meet to decide on recommendations for corrective measures or enhancements for areas where test results have been unsatisfactory. The individual test results should be reviewed by the entire team. In some instances, security enhancements may resolve the inadequacy of multiple controls. For example, it may have been discovered that the names of departed personnel are still being carried on the computer-facility access records. The implementation of adequate check-out procedures for terminating employees will correct the deficiency.

When the team has completed its analysis and developed its recommendations, a copy of the findings should be forwarded to each manager concerned as well as to top management. Such reporting should be considered highly sensitive and confidential and should be stringently controlled. The database should be updated to reflect the current status of each deficiency discovered during testing. [Ref. 27:p. III-1-4] There are two basic installation strategies that could be followed. The first is the pilot strategy. Such a strategy involves installing the controls on a selected segment of the IS. For example, it may prove advisable to install the controls application by application. This approach could prove time consuming but it could isolate the damages in case the new controls prove to be a problem. A second strategy involves a phased approach. For example, data entry or data processing controls could be installed in phases over a select period of time. This approach could prove effective if the data entry or data processing controls are considered highly complex and difficult to install. Therefore, it becomes more prudent to break down the installation of the controls in more manageable phases. [Ref. 33:p. 111]

D. SYSTEM MANAGEMENT

1. System Organization

There are three issues which should be addressed regarding the organization of an IS security system. First, there is the issue of the appropriate system configuration. As indicated in Chapter III, the system can be configured in either a centralized or decentralized manner. The appropriate security system configuration is the one that corresponds to the manner in which IS resources and components are structured and deployed within the organization. In other words, if IS resources and components are centralized then IS security controls should be deployed to correspond with it.

The second issue concerns the placement of the security manager's position within the organization. It is of the utmost importance that the position be as independent as possible. The matter of independence becomes even more critical as the organization's level of dependency and the value of its IS assets rise. It would seem that the best means of achieving such independence is to have the security manager accountable to the highest official in the organization (e.g., the chief executive officer, chairman of the board, director). Another approach is to have the security manager accountable to a governing body (e.g., board of directors, trustees) or a subdivision of such a body (e.g., audit committee, security committee). Also, such higher authorities

would be responsible for such items as approving the appointment of an individual to such a position, approving the IS security budget and annual security plan, approving the salary and performance appraisal of the security manager, and the approval of all test results.

The third issue involves the number of organizational units that are in a reporting relationship with the security manager and his staff. It is important that there be open established lines of communication between the security manager and the classification review committee; IS management; top management; users; and the internal audit staff. One means of achieving an effective working relationship between all the parties is to establish a permanent security committee. This committee would meet on a regular basis to discuss security issues and to establish security policy.

2. **Security Planning**

Security planning involves several significant activities. First, both short range and long range planning should be performed. Short range planning is essentially operational in nature. That is, it is responsible for planning the implementation of the annual security plan. Second, long-range planning should be established. Such planning seeks to anticipate or project future threats and vulnerabilities to the IS. Both types of planning should be highly coordinated with IS planning activities.

3. **Security System Staffing**

There are several issues in regard to the staffing of the security system. First, security staff salaries, promotions, and performance evaluations should be determined by the security manager as much as possible with the approval of the highest levels of management. This is necessary to maintain the independence and objectivity of the IS security staff. Second, security staff personnel, even those who work within a decentralized security system configuration, should report directly to the organization's IS security manager. Once again, this is to maintain the elements of objectivity and independence. Finally, due to the dynamics of IS technology, it is critical that the security staff be provided with appropriate IS security training. The staff should maintain a library of professional books and periodicals.

4. **Security System Monitoring and Evaluation**

The security staff is responsible for the monitoring, investigation, and reporting of the security system's performance. This is accomplished in several major ways. First, the staff can attempt violations at different times and at different levels within the IS. The purpose of the violations is to determine if the system responds to

such violations in the required time and manner. Second, various kinds of scenarios and drills can be performed to train users and to test the installed controls. Examples include disaster recovery and fire drills. Third, selected user actions could be monitored and investigated to determine if such actions were within their authority. Examples of such actions would involve data update, transfer, and destruction, especially of data previously classified as extremely critical and extremely sensitive.

5. **Security Components (Tasks)**

A structure will need to be formed to perform the security tasks that were discussed in Chapter III, Section C. These tasks involve avoidance, deterrence, prevention, detection, and recovery and correction. Depending on the scope of security responsibilities, separate departments (or divisions) could be formed for each task. For example, the security staff would have a separate department that is only responsible for various kinds of recovery and correction programs (e.g., contingency plans, off-site back-up, on-site back-up). If the scope of the security staff's responsibilities are more limited due, for example, to an organization being at a lower level of IS dependency, then several of the tasks could be combined in one department. For example, one department could be responsible for recovery and correction as well as preventive programs (e.g., personnel screening, external labels, protect rings for magnetic tapes).

6. **The Security Database**

During the course of the planning, design, installation, and testing of the security system, various items of information were entered into what was defined as a security database. This information will serve as a basis for effectively managing and maintaining the security system. A description of the contents of the database is contained in Appendix L.

It is important that the information contained within the database be updated, expanded, or reduced as circumstances within the organization and its environment changes. The database provides a means for recording and analyzing such changes and for planning appropriate responses. By doing so, it provides a valuable decision support tool that should be centrally maintained and controlled by the security staff.

There are some significant changes which will affect the database which warrant a brief discussion. First, new laws may be passed which could require the installation of new controls on assets. Also, as an organization expands it operations, it may deploy facilities and people overseas and into different parts of the U. S. This could subject the organization to whatever security-related laws exist within these areas.

Second, changes can occur to the inventory of assets. If assets are added, then the process of classification, threat identification, impact analysis, vulnerability assessment, logical design, practical design, and implementation should take place. On the other hand, if assets are deleted from the inventory, the controls which are applied to protect them should be removed when considered necessary.

Third, the classification program results may have to be changed. Circumstances may require either increasing or decreasing the classification levels of various applications, data, and transactions. Such changes could be caused by the growing significance or insignificance of an application, such as a customer service system, to the organizations operations.

Fourth, the type and probability of various threats could change over time. As new assets are added to the organization's inventory, the events which pose threats to such assets should be determined and studied. The probabilities of the occurrences of these threats will change over time based on historical experiences and the results of various tests.

Fifth, there will be changes to the results of impact analyses. Such changes are caused by changes in the costs of replacing and correcting the impacts caused by the threats.

Sixth, an organization's state of vulnerability changes over time. This state is essentially an indication of the organization's level of protection over its assets at any given point in time. As the combination of assets, threats, and controls changes over time, so does the state of vulnerability. One measure of the performance of the security staff is how material the vulnerability state is at any given point and the length of time that such a state has existed. The materiality of the state could be measured by the number of vulnerabilities which pose the greatest threats to those applications, data, and transactions which were classified as extremely sensitive and extremely critical. The results of the various testings, monitorings, and audits provide additional information which would help determine the state of the IS vulnerability and provide a means to assess its performance.

E. CONCLUSIONS

This phase resulted in the installation and testing of the controls which were selected during the design phase. Also, a structure, components (tasks), procedures, people, and information were combined to provide an overall management for the

developed security system. The system's management has two significant responsibilities. First, it is responsible for ensuring that the established security system is performing in an effective and efficient manner. Second, the security system management is responsible for ensuring that the system appropriately responds to both internal and environmental changes which affect it.

VII. CONCLUSIONS

This new development (automation) has unbounded possibilities for good and for evil. [Norbert Wiener]

This thesis is ended the way it was started. That is, with a statement about the potentials for both the good and bad that could result from the unleashing of automation technology upon society. Just as the unleashing of the power that fuels the stars has had ever growing consequences upon the way man lives, so too has the unleashing of the physical and logical properties that can manipulate and communicate pulses of electricity. The good of automation technology has been present from the beginning of its infusion within the society. It has only been in recent years that the dangers and problems have been given greater attention. It is in response to these dangers and problems that IS security arises as an issue. It embodies two of the basic principles of our democratic society. That is, the need for appropriate checks and balances and that unlimited power could eventually lead to the limitation of human rights and freedoms. The infusion of automated technology has grown ever rapid and wider. This thesis offered a brief description of just how wide and rapid the applications of the technology have become throughout society and some of the dangers which have resulted.

This thesis also offered a means of viewing computers in a much broader and more refined context than that usually offered. The approach offered involved addressing the subject of computers from the context of a "system". The conventional definition of a computer system narrowly defines it as consisting of hardware, software, people, data, and procedures. However, within the broader context of a "systems approach", these items would only just represent the resources part. The remaining parts involve the objectives, environment, components (tasks), and the management. Within this framework, an "information system" is defined. The same approach was followed to construct a framework for a security system.

As a means of constructing an IS security system within this framework, a three phased generic development model was presented. The planning phase of the model establishes security policy (objectives and priorities); determines the extent of security

requirements; identifies assets requiring protection; and classifyies the assets based on their level of criticalness and sensitivity. This classification forms the basis of the subsequent design of controls which will be applied to the assets to provide the necessary protection. This design of controls involves an initial identification of threats and their probable economic impacts to the assets. The current state of protection provided to the assets is subsequently assessed. A configuration of controls is constructed to remedy any established security weaknesses. The implementation phase provides the testing and installation of the controls which are needed to actually link the IS security system with the IS. A management structure is established to maintain and improve the developed security system.

It is believed that the thesis offers a definitional framework and development model of sufficient substance so as to serve as a basis for the performance of security system developments within a broad range of organizations. The depth and scope within each phase will vary by its application to a wide range of organizational situations. However, the basic concepts of asset identification, definition, and classification; threat identification; impact analysis; vulnerability assessment; and the cost-benefits of controls should remain stable enough to provide a basis for the model's change and continued use over time. An organization's need for this model or any other security system development and management approach will be substantially increasing over time. The causes for this increasing need lie outside and within an organization.

There is a rising public awareness and concern with the issues of IS security. The political institutions are responding more and more with laws which address these issues. For example, at the time of this writing, the Congress of the U. S. approved the Computer Fraud and Abuse Act of 1986. [Ref. 42:pp. 1 & 8] If signed by the President, as expected, the act will expand federal jurisdiction to cover interstate computer crimes in the private sector. The act would make it a federal misdemeanor to traffic in stolen passwords with intent to defraud or to intentionally trespass in a "federal-interest computer" to observe or obtain data. It would be a felony to access such a computer for a theft-by-computer scheme or to alter or destroy computer data - if the victim suffers a loss of at least $1,000 or if the files are medical records - without authorization. Also passed by the Congress and awaiting the President's signature is the Electronic Communications Privacy Act. This act would change and update the 1968 Federal voice-oriented wiretap law to reflect dramatic changes in computer and

communications technologies, including the expansion of electronic mail and development of computer networking. It would make it illegal to access electronic messages without authorization. On an international scale, there are efforts underway to control transborder data flow (TBDF), or the transmissions of electronic information across national borders. The protection of the content of the information being transmitted is a major issue that is under discussion. [Ref. 43:p. 37] It is believed that this continued public awareness and regulation will be increasing the mandatory IS security responsibilities of organizations. This will require increased internal expenditures for IS security.

Also, as organizations come to rely more and more on computer technology for basic operational needs as well as to support the achievement of strategic objectives, there are increasing pressures to protect their IS assets. This increasing reliance on computer technology is reflected in rising levels of dependency which was previously discussed. Both the external and internal pressures faced by organizations to provide adequate IS security makes it increasingly essential that they have an orderly, well-defined approach for developing, operating, and managing a system which can meet their security requirements.

APPENDIX A

IS ASSETS

1.0 FACILITIES. These include a data center's physical plant and its supporting devices and utilities.

1.1 Physical Plant. Actual structure in which data processing and communications are housed including auxiliary buildings such as PBX areas, generator buildings, cooling towers.

1.2 Electrical Power Systems. Transformers, wiring, generators, power filters, uninterruptible power sources, emergency/backup power units.

1.3 Environmental Support Systems. Air conditioning compressors, dehumidifiers, air-handling units, ductwork, water chilling units, thermostats, humidistats, plumbing, air intake equipment.

1.4 Fire Detection and Suppression Systems. Smoke/heat detectors annunciator panels, alarms, Halon 1301/1211, CO2, water sprinkler systems.

1.5 Intrusion Detection and Alarm Systems. Motion detectors, magnetic contact switches, vibration sensors, annunciator panels, alarms, closed-circuit television and videotape recording units, facility access control monitoring systems.

2.0 Hardware. This includes all data processing and communications hardware.

2.1 Central Processing Unit. Main memory, cache memory, arithmetic logic unit, channels, operating console, system disk, associated peripheral processing units.

2.2 Magnetic Storage Devices. Magnetic disks (including floppies), tape, drum.

2.3 Local Input/Output Devices. Printers, card readers, MICR readers, local terminals, COM units.

2.4 Communications Controllers. Auxiliary processors placed between CPU and transmission facilities to handle such functions as line management and code translation.

2.5 Modems. Devices translating signals between input/output devices and communications lines.

2.6 Terminal Concentrators. Devices that link multiple channels to allow use of common transmission channels.

2.7 Digital Switches. Devices designed to create or break a physical communications circuit, generally within a network control center.

2.8 Remote Input/Output Devices. All input/output devices on distal (outbound) side of model (e.g., remote terminals).

2.9 Cryptographic Devices. Devices designed to encrypt or scramble voice or data transmissions, rendering them unintelligible if intercepted by unauthorized persons; a compatible device decrypts messages into intelligible form at receiving end.

2.10 Multiplexors. Devices that take a number of communications channels and combine signals into one common channel for transmission; at receiving end, demultiplexor separates signals.

2.11 Local Loop. Communications circuit between user location and telephone company central office.

2.12 Terrestrial Microwave Circuits. All proprietary terrestrial microwave communications circuits and facilities maintained and operated by user for local or long haul communications.

2.13 Satellite Circuits. Proprietary satellite communications circuits and facilities, such as earth stations and antennas, operated by user for point-to-point satellite transmission.

3.0 Software. This group of assets includes all systems and applications software and chips used by the mainframe and distributed processors.

3.1 Operating Systems. Systems software (generally vendor supplied) that performs job control/scheduling, input/output control, interrupt, file maintenance, high-level language support (compilers/assemblers), memory allocation, logging of system activities (e.g., MVS, OS/MVT, GCOS).

3.2 Data Base Management Systems. All software necessary to develop, use, maintain data base systems (e.g., IMS, IDMS, IMAGE).

3.3 Communications Control Software. Software contained in either host processor or a network frontend communications controller that controls such functions as message switching, line monitoring/control, message parity/error checking, handshaking, line allocation.

3.4 Security Software. Software designed to conduct extended access checking beyond that performed by communications software or operating system, to restrict access to protected resources, and to monitor line activity.

3.5 Applications Software. All user-oriented software developed in high-level languages and running under supervision of operating system.

4.0 Data. Data can be defined in three broad groups.

4.1 Financial Data. Checking account balances, accounts payable/receivable, funds transfer balances.

4.2 Proprietary Data. Sensitive business data (trade secrets), sensitive non-business data (personnel records, salary levels), restricted records (tax records, public assistance information, other records restricted by law or regulation).

4.3 Personal Data. Personnel records (pay, performance), credit records; medical records, educational records, all records covered by state and federal privacy laws.

5.0 People. There are seven groups of people.

5.1 Computer Operator. Operates computer from console; alters job schedules/priorities, initiates program execution, responds to system error messages, mounts/demounts magnetic media.

5.2 Data Entry Clerk. Operates remote terminal; enters transactions, data, programs.

5.3 Media Librarian. Files, retrieves, accounts for offline storage of data/programs on removable magnetic media; provides media to production control, cycles backup to remote facilities.

5.4 System Programmer. Designs, develops, installs, documents, maintains operating systems, DBMSs, communications software, system accounting features, security software packages.

5.5 Application Programmer. Designs, develops, installs, documents, maintains user programs and application systems.

5.6 IS Security Manager. Plans, implements, installs, operates, maintains, and evaluates physical, operational, technical, procedural, personnel-related controls.

5.7 IS Auditor. Performs operational, software, and data file reviews to determine adequacy, performance, security, compliance with organizational policy, procedures, standards; participates in design specification of applications to ensure adequacy of controls.

SOURCE: Ref. 26: pp. II-3-1 to II-3-3.

APPENDIX B

SENSITIVITY CLASSIFICATION LEVELS

	Sensitivity Level A	B	C	D	E	F
Competitive Data The willful or inadvertent release or disclosure of this data could result in a competitor being given a significant business advantage over the organization. The effect of such disclosure on the bottom line could be:						
5 = More than $10,000,000	X					
4 = $1,000,000-$10,000,000		X				
3 = $100,000-$1,000,000			X			
2 = $10,000-$100,000				X		
1 = Up to $10,000					X	
0 = None						X
Data with Fraud Potential Unauthorized modification of accounting or authorization data that controls the disbursement of funds could result in a fradulent disbursement of:						
5 = More than $10,000,000	X					
4 = $1,000,000-$10,000,000		X				
3 = $100,000-$1,000,000			X			
2 = $10,000-$100,000				X		
1 = Up to $10,000					X	
0 = None						X
Privacy Data Personal data directly traceable to an individual either is covered under federal, state, or local privacy legislation or is considered company private. This data consists of:						
5 = Personal/Health/Credit Data	X					
4 = Financial/Account Balance Data		X				
3 = Salary/Performance Data			X			
2 = Name/Address Data				X		
1 = Other					X	
0 = None						X

Note:

A = Extremely Sensitive	=	5
B = Highly Sensitive	=	4
C = Sensitive	=	3
D = Moderately Sensitive	=	2
E = Minimally Sensitive	=	1
F = Nonsensitive	=	0

SOURCE: Ref. 26: p. I-E-3.

APPENDIX C

CRITICALNESS CLASSIFICATION LEVELS

Criticalness	Criticalness Level G	H	I	J	K	L
The availability and accuracy of this data have the following effect on overall application operation:						
5 = System cannot operate without it.	X					
4 = System would be seriously impaired to the point where its usefulness would be questionable.		X				
3 = System operation would be degraded; however, main functions would be useful or available.			X			
2 = System would experience some impact; however, all functions would be usable or available with somewhat degraded response times.				X		
1 = System would be minimally impacted by loss of this data; loss would occasion no operational degradation					X	
0 = No impact.						X

NOTE:

G = Extremely Critical	=	5
H = Highly Critical	=	4
I = Critical	=	3
J = Moderately Critical	=	2
K = Minimally Critical	=	1
L = Noncritical	=	0

SOURCE: Ref. 26: p. I-E-4.

APPENDIX D

SENSITIVITY/CRITICALNESS MATRIX

	Competitive Data	Data With Fraud Potential	Privacy Data	Criticalness
0	F	F	F	L
1	E	E	E	K
2	D	D	D	J
3	C	C	C	I
4	B	B	B	H
5	A	A	A	G

NOTE:

A = Extremely Sensitive = 5
B = Highly Sensitive = 4
C = Sensitive = 3
D = Moderately Sensitive = 2
E = Minimally Sensitive = 1
F = Nonsensitive = 0
G = Extremely Critical = 5
H = Highly Critical = 4
I = Critical = 3
J = Moderately Critical = 2
K = Minimally Critical = 1
L = Noncritical = 0

0-5 = Sensitivity/Criticalness Levels

SOURCE: Ref. 26: p. I-E-11.

APPENDIX E

THREATS

A.0 NATURAL THREATS

A.1 **Threat:** Internal flooding

Examples:

- Water or steam pipes in walls or ceilings adjacent to the data center burst, causing flooding and/or corrosion from water and steam.
- Water chiller pipes used for equipment cooling burst or leak, flooding and/or shorting electrical components.
- The sewer system serving adjacent lavatory facilities backs up, spilling water and sewage into the data center.
- A wet-pipe sprinkler head in the computer room malfunctions or is accidentally knocked loosed, discharging high-pressure water into the data center.

A.2 **Threat:** External flooding

Examples:

- Runoff from rains accompanying hurricanes or other storms overloads storm drains, flooding below-ground-level data centers.
- Rooftop cooling towers for air conditioning on water storage tanks for fire suppression burst or leak, flooding floors beneath them.
- Coastal or lakefront areas are flooded by tsunami or tidal wave activity.
- Water buildup on flat roofs leaks into lower floors.

A.3 **Threat:** External fire

Examples:

- Fire in another part of the facility housing the data center spreads to the equipment area or makes access to the data center impossible.
- Fire in the supporting utility area is carried by the air-handling system to the DP area.
- Fire in the building's electrical system, while not directly involving the data center, makes the data center inoperable through loss of power.

A.4 Threat: Internal fire

Examples:

- Improperly installed wiring in wiring closets or under raised flooring starts a fire.
- Careless use or storage of combustible materials, such as paint, solvents, or cleaners, results in fire.
- Careless use of matches, lighters, or smoking materials ignites flammable materials--paper stock, plastics, and oxide-based materials, such as magnetic tapes and disks.

A.5 Threat: Seismic damage

Examples:

- Even relatively small tremors cause head crashes or other vibrational damage.
- Tremors cause structural failure, resulting in the collapse of walls, ceilings, and floors (even small tremors can do this to internal construction, such as raised floors and suspended ceilings, within the data center).
- Seismic vibration causes bursting of water pipes, damage to HVAC equipment, and disruption of electrical service.

A.6 Threat: Wind damage

Examples:

- Hurricanes or tornadoes may cause structural failure of the facility, resulting in major damage to system components.
- In facilities with exterior windows, the sudden cyclonic low pressure associated with tornadoes shatters windows with explosive effect, causing severe injury to personnel and serious damage to equipment.

A.7 Threat: Snow and/or ice storms

Examples:

- Excessive snow accumulation on rooftops causes structural collapse.
- Ice accumulation on power supply causes cable failure, resulting in power outage.
- Impassable roads prevent essential personnel from reporting for normal work schedule.

B.0 ACCIDENTAL THREATS: TECHNICAL

B.1 Threat: Power failure/fluctuation

Examples:

- Facilities without adequate power conditioning (filtering) experience equipment damage or destruction of data as the result of spikes or surges caused by the introduction of large quantities of additional power, such as lightning strikes.
- The power utility experiences total failure.
- Facilities with inadequate uninterruptible power sources experience data loss during power reductions (brownouts) by the utility.
- The internal distribution system (e.g., transformer) fails, denying the facility electrical power.

B.2 Threat: Heating, ventilating, air conditioning failure

Examples:

- Environmental control systems malfunction, causing the temperature in equipment areas to exceed safe ranges for operation, resulting in erratic equipment performance, damage to equipment and data, for fire.
- Improper or inadequate preventive maintenance of HVAC equipment (e.g., failure to change filters or to recharge freon) causes erratic performance of equipment failure.
- HVAC systems have inadequate capacity to handle periodic extremes of temperature or humidity.
- System enhancements made without adequate consideration to existing HVAC capacity cause degradation of service or failure from system overload.

B.3 Threat: Failure of communication circuits

Examples:

- Circuits are physically destroyed by natural disaster or vandalism.
- Excessive noise or crosstalk on telephone company lines garbles messages during transmission.
- Natural phenomena (e.g., sunspots) disrupt microwave and satellite communications.
- Excessive demand for existing circuits causes queuing and routing problems.
- Malfunction or failure of switching hardware at telephone company central office causes failure to establish switched circuit or misrouting of message traffic.

B.4 Threat: Failure of communications hardware/firmware

Examples:

- Failure of switching in a store-and-forward network results in lost message traffic.
- Failure of communications controllers, modems, cryptographic devices, or digital switches causes service denial.

B.5 Threat: Failure of communications software

Examples:

- Software in a network front-end processor fails during authentication, data validation, error detection/correction, polling, or other activity, resulting in errors, lost or changed messages, or service denial.

B.6 Threat: Malfunction or failure of CPU, mass storage, or I/O devices

Examples:

- Malfunction or failure of system hardware components during input, processing, or output destroys critical data or denies service to system users.
- Inadequately trained operators damage critical components.
- Improper/inadequate maintenance causes hardware failure.
- Hardware delivered by the vendor does not perform to specification or fails because of improper manufacture or installation.
- Performance characteristics and reliability have been misrepresented by vendor.

B.7 Threat: Malfunction or failure of systems software

Examples:

- Operating systems, data base management systems, and the like malfunction or fail, causing modification of data, lapse of system control, or service denial.
- Local system programmers improperly design enhancements to systems software.
- Vendor-released software changes are improperly installed and inadequately tested prior to operational use.
- Attempts by users to circumvent access control mechanisms cause operating system to crash.

B.8 **Threat:** Malfunction or failure of applications software

Examples:

- Application packages inadequately tested prior to implementation allow logical errors to be introduced to operational systems.
- Changes are made to applications without a concurrent change to user documentation, run books, and job setup procedures, causing program errors.
- Poor logical design of software (because of inadequate specification and program verification) results in program malfunction or failure.

B.9 **Threat:** Electromagnetic interference (EMI)

Examples:

- Radio transmitters and radar units (both ground and airborne) in the proximity of the facility interfere with operations.
- The introduction of televisions, CB radios, and other electronic equipment into the data center changes bit configurations in core.
- Static electricity from carpeting causes accidental erasure of data on magnetic media.

B.10 **Threat:** Electromagnetic emanations

Examples:

- Conventional telephone instruments, lamps, radios, and other electrical devices act as transmitters and radiate electromagnetic signals.
- Improperly grounded equipment, electrical junction boxes, and cable troughs turn the entire building into an antenna for the transmission of signals.

C.0 **ACCIDENTAL THREATS: HUMAN**

C.1 **Threat:** Data entry error

Examples:

- Careless data entry operators miskey data during input.
- Careless handling of source documents results in dual entry of the same transaction.
- Data entry operator fails to enter data from a source document.
- Entry errors cause processing errors, halts, or output errors.

C.2 Threat: Improper handling of sensitive data

Examples:

- Source documents for sensitive transactions (e.g., check posting, authorization of payment vouchers) are inadequately safeguarded to prevent fraudulent modification or substitution prior to entry into the system.
- Passwords/user IDs are not properly safeguarded: they are written on a terminal or desk blotter, passed to other users for convenience, and so on.
- Data control clerks do not require that all output be signed for by the user.
- Sensitive output or tapes are left unattended in offices, reception areas, or terminal rooms.

C.3 Threat: Unauthorized physical access

Examples:

- Laxity or lack of training on the part of data center personnel permits access to the facility by unauthorized personnel.
- Visitors are not properly escorted while in the facility.
- Maintenance personnel and vendor representatives who frequently visit the facility are allowed unescorted access (even though this is not authorized).
- Former employees retain or obtain possession of combinations, keys, magnetic access cards, and other means of access.

C.4 Threat: Accidental damage to hardware, software, or data

Examples:

- Inexperienced or careless operators clear memory locations without properly backing up data or programs.
- Operators attempt to fix abends on production shifts without calling software support personnel, damaging production programs or data.
- Inexperienced or improperly trained programmers use systems software "hooks" to enter supervisor state to apply quick fixes to software problems, damaging systems software or data.

D.0 MALICIOUS THREATS

D.1 **Threat:** Malicious damage/destruction of physical assets

Examples:

- Radical group destroys the data center for ideological reasons.
- Data center is vandalized.
- Disgruntled employee seeking vengeance destroys or sabotages system resources.

D.2 **Threat:** Malicious damage/destruction of software or data

Examples:

- Software or data is damaged or destroyed as part of a planned assault on system resources or as random vandalism.
- Disgruntled employee erases data files and/or program files.
- System penetrators destroy data files.

D.3 **Threat:** Unauthorized access to data/theft of data

Examples:

- System programmers, operators, auditors, managers, or other persons in sensitive positions circumvent access control procedures to obtain information for their own benefit or that of a third party.
- Penetrators successfully circumvent access control mechanisms and gain access to sensitive data files.
- Sensitive data transmittal in unencrypted form is monitored and its content made available to unauthorized persons.
- A program masquerades as the log-on subroutine and illicitly obtains passwords and user IDs.
- Programs mimic device identification of legitimate output devices (CRTs, printers, etc.), causing restricted data to be output to unauthorized devices.

D.4 **Threat:** Unauthorized modification of software of hardware

Examples:

- A "trapdoor" program is inserted in systems software to bypass operating system controls and allow clandestine entry into supervisory mode while simultaneously suppressing any record of mode entry.
- A "Trojan horse" code module is inserted in a critical application program to perform an

unauthorized act (e.g., credit an account, disregard a debit entry, write a check) without appearing on the audit trail.
- Firmware security modules are covertly replaced with modules that negate firmware implementation of security controls.

D.5 Threat: Fraudulent generation or modification of data

Examples:
- Data is modified to cover evidence of poor performance, incompetence, or prior illicit behavior.
- Sales figures are inflated to increase performance statistics.
- Inventory is understated for purposes of tax evasion.
- Assets are overstated for purposes of manipulating a loan application.
- Data is modified to conceal bribery of an official or other illegal activities.
- Fraudulent payments are generated.

SOURCE: Ref. 26: pp. II-2-1 to II-2-17.

APPENDIX F

THREAT/ASSET MATRIX

Threats	Assets
A.1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11
A.2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.1, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11
A.3	All assets threatened
A.4	All assets threatened
A.5	1.1, 1.3, 2.1, 2.2, 2.4
A.6	1.1, 1.3
A.7	1.1, 1.2, 1.3
B.1	1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10
B.2	1.3
B.3	2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13
B.4	2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10
B.5	2.4, 2.6, 2.8, 3.3
B.6	2.1, 2.2, 2.3, 2.8
B.7	3.1, 3.2, 3.4
B.8	4.1
B.9	1.1, 1.5, 2.2, 2.11, 2.12, 2.13, 3.1, 3.2, 3.3, 3.4, 3.5
B.10	1.1, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9
C.1	3.5, 4.1, 4.2, 4.3, 5.2

C.2	2.2, 2.3, 2.8, 2.11, 2.12, 2.13, 4.1, 4.2, 4.3, 5.1, 5.2, 5.2, 5.4, 5.5, 5.6, 5.7
C.3	All assets threatened
C.4	2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 3.1, 3.2, 3.3, 3.4, 3.5, 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7
D.1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7
D.2	3.1, 3.2, 3.3, 3.5, 3.5, 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7
D.3	1.5, 2.2, 2.3, 2.8, 2.11, 2.12, 2.13, 3.1, 3.2, 3.3, 3.5, 4.2, 4.2, 4.3
D.4	2.1, 2.4, 2.8, 3.1, 3.2, 3.3, 3.4, 3.5, 5.1, 5.4, 5.5
D.5	2.3, 2.4, 2.8, 2.11, 2.12, 2.13, 3.5, 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7

SOURCE: Ref. 26: p. II-3-5.

APPENDIX G

ORDERS OF MAGNITUDE OF ESTIMATED IMPACT AND FREQUENCY

IMPACT:

$10,	let i = 1
$100,	let i = 2
$1000,	let i = 3
$10,000,	let i = 4
$100,000,	let i = 5
$1,000,000,	let i = 6
$10,000,000,	let i = 7
$100,000,000,	let i = 8

FREQUENCY:

Once in 300 years,	let f = 1
Once in 30 years,	let f = 2
Once in 3 years,	let f = 3
Once in 100 days,	let f = 4
Once in 10 days,	let f = 5
Once per day,	let f = 6
10 times per day,	let f = 7
100 times per day,	let f = 8

SOURCE: Ref. 43: p. 3E-7.

APPENDIX H

COMBINED MATRIX OF I, F, AND ALE

Impact (i)	Frequency (f)							
	1	2	3	4	5	6	7	8
1					$300	$3,000		$300k
2				$300	$3,000	$30k	$300k	$3M
3			$300	$3,000	$30k	$300k	$3M	$30M
4		$300	$3,000	$30k	$300k	$3M	$30M	
5	$300	$3,000	$30k	$300k	$3M	$30M	$300M	
6	$3,000	$30k	$300k	$3M	$30M	$300M		
7	$30k	$300k	$3M	$30M	$300M			
8	$300k	$3M	$30M	$300M				

SOURCE: Ref. 43: p. 3E-8.

APPENDIX I

SECURITY RESOURCES (CONTROLS)

PHYSICAL SECURITY CONTROLS

1. Electronic Access Control Systems (EACs)

Install electronic systems to control and monitor physical access to all restricted areas within the data center. These systems generally consist of a small CPU containing access control tables, which journals and records access information, plus personal identification and authentication (PI&A) devices that identify users to the system. Among the PI&A technologies currently used as part of EACs are the following:

- 1.1 · Magnetic card/badge readers--These mediate access based on reading a magnetically encoded badge or card; often used in conjunction with electronic cipher pads and other PI&A technologies. Procedures for the control of cards and badges should be developed.
- 1.2 · Biometric devices--These devices measure certain physical characteristics of an individual; they include hand geometry readers, fingerprint analyzers.
- 1.3 · Voice Recognition Units--Digitized voice input is compared with stored digital voice signature data.
- 1.4 · Signature Analysis--Stored digitized handwriting sample is compared with signature obtained from user when entry is desired.

2. Intrusion Detection Systems (IDSs)

Use these devices to detect and monitor unauthorized entry into restricted areas. IDSs use several technologies that are suited to particular protection situations.

- 2.1 · Passive infrared--The presence of intruders is detected from the thermal radiation emitted by the human body. Use for surveillance of doors, windows, and enclosed areas.
- 2.2 · Active infrared--Infrared beam is projected across area to contact a light-sensitive cell; hidden mirrors allow the beam to crisscross the area. Movement is detected by a break in the beam. Use for surveillance of passage ways, other large areas.
- 2.3 · Ultrasonic systems--These flood an area with ultrasonic radiation and detect intruders from

changes in wave patterns. Use for large enclosed areas.

2.4 · Sonic systems--Sensors installed on walls, ceilings, floors detect any sounds in enclosed areas. Use where there is a minimum of extraneous noise.

2.5 · Magnetic contacts--Contact alarms form an electrical circuit. Breaking the circuit (as in opening a door or window) activates an alarm. Use on doors, windows, file cabinets.

2.6 · Vibration sensors--These detect vibrations caused by breaking glass or attempts to break through a wall, floor, or ceiling.

2.7 · Microwave systems--Similar to ultrasonic systems, these systems emit high-frequency radio waves that are transmitted by and partly reflected back to antenna. The frequency changes when the waves strike a moving object.

3. Electromagnetic Interference (EMI) Prevention

High-energy electromagnetic radiation, such as that given off by TV transmitters, microwave equipment, and high-powered UHF/VHF transmitters, may alter bit settings in core or change data stored on magnetic media. Precautions should be taken to prevent damage from EMI by:

3.1 · Locating equipment away from high-energy sources.

3.1 · Proper grounding of all equipment.

3.3 · Exclusion of radios, TVs, microwave ovens, and other non-DP-related electronic devices from equipment areas.

4. Fire Detection and Alarm Systems

All DP facilities should be equipped with adequate fire detection and alarm systems, as specified by National Fire Protection Association (NFPA) Standard 75[4]. Two basic technologies are used:

4.1 · Smoke detectors--Photocell or ionization-type devices should be installed in:
--Equipment areas
--Spaces above false ceilings
--Areas beneath raised flooring
--Tape libraries
--Forms and supply storage areas
--Office areas and passageways

4.2 · Heat detectors--Two types are generally used: rate-of-rise and temperature threshold. Rate-of-rise detectors should be installed in:
--Areas beneath raised flooring
--Electrical closets and in electricity-generating areas
Temperature-threshold sensors should be used in:

--Tape libraries
--Forms and supply storage areas
--Office areas and passageways

All detectors should be integrated with an alarm system that is visible as well as audible. Alarm annunciation should be both local and at a fire station or central fire/security control center.

5. Fire Suppression Systems

All facilities should have both automatic and manual fire suppression systems:

- Automatic systems--These are activated automatically as a result of detector activation:
  - 5.1 Water sprinkler--Provides continuous suppression as long as water source is available. Only dry-pipe systems, which are not charged with water until a heat/fire/smoke detector is activated, should be used.
  - 5.2 Halon 1301--One-shot systems with no continuous suppression after initial; eliminate danger of water damage.
  - 5.3 CO_2--Not for use in areas where personnel are present. Effective for under-floor suppression or in areas with potential for electrical fires (e.g., electrical closets, generator areas).
  - 5.4 Manual systems--Hand-held extinguishers of CO_2 or Halon 1301 or 1211.

6. Emergency Power

Equip the facility with battery- or automatic generator-driven emergency power. System capacity should be sufficient to power the following minimum essential systems for 48 hours:

- Electrically activated door locks.
- Fire detection and suppression systems.
- Intrusion detection and alarm systems.
- Intercoms and internal telephone systems.

7. Emergency Lighting

Equip facility with battery- or automatic generator-powered emergency lighting in the data center, passageways, and stairwells, and at all emergency exists. All units should begin immediate operation when power fails and allow sufficient time for an orderly evacuation of the facility.

8. Facility Location

The physical location of a facility, both geographically and within a larger structure, can have a major effect on its overall security. In locating DP facilities, consider the following factors:

- Geographic
  --Out of floor plains, earthquake zones, landslide areas, hurricane or typhoon zones, and tornado-prone areas.
  --Away from high-crime areas.
  --Away from high levels of high-frequency microwave or radio transmissions (e.g., airports, microwave relay sites).
  --Far enough away from highways, railways, and heavy construction to avoid damage from vibration.
  --Away from flammable or explosive material storage areas.
- Location within a structure
  --Above ground level.
  --Below the top floor.
  --In the interior of the building away from exterior windows.

9. Facility Construction

Construct the DP facility in accordance with existing fire and occupational health and safety standards. Pay particular attention to ensuring that:

- The facility is constructed of fireproof material in accordance with the National Fire Code, NFPA 70[4].
- The facility is windowless, or existing windows are secured with steel screening or louvers, and all are alarmed.
- The facility has adequate emergency exits and egress signalling in accordance with NFPA standards [4].
- The facility uses architectural features such as man-traps and single access points to enhance overall security.
- The facility provides adequate space for proper equipment installation, cable troughs, ducting, and other adjuncts of data processing.

10. Housekeeping Standards

Maintain basic standards of housekeeping within the data center.

- Prohibit eating, drinking, and smoking in equipment and forms of storage areas.
- Keep the area under the raised flooring clean and free of dirt and trash.
- Empty trash receptacles regularly.
- All DP personnel should be held responsible for a clean working environment.
- Supervisors should periodically inspect areas for adequate housekeeping.

11. HVAC Systems

Because heating/ventilating/air conditioning systems are crucial to the basic functioning of DP department, certain basic steps must be taken to ensure the uninterrupted functioning of these systems. These steps should include:

- Regular maintenance of all HVAC equipment.
- Multiple heat-pump/chiller units with sufficient capacity to provide backup in case of unit failure.
- Use of HVAC systems dedicated to DP operations--not supporting any other functions within the facility.
- Temperature/humidity alarms to warn of environmental control problems.

12. Closed Circuit Television (CCTV)

CCTV used in conjunction with video tape recording (VTR) equipment is a powerful security monitoring tool and an effective deterrent. Useful CCTV for surveillance of:

- Unattended terminals and other sensitive equipment.
- Facility entranceways.
- Internal passageways and stairwells.
- Supporting utilities (e.g., HVAC areas, telephone wiring closets).

In multiplexed systems (using more than one camera per monitor), ensure that the camera-to-monitor ratio does not exceed five to one. If cameras are not constantly monitored by guard force personnel, they should be equipped with VTRs at a ratio of no more than five to one.

13. Uninterruptible Power Supply (UPS)

Provide an uninterruptible power supply of sufficient capacity to allow for graceful system shutdown in the event of power failure, through use of:

- A battery system that provides enough time to dump files and bring the system down.
- A combination battery/generator system, in which the battery provides sufficient backup until the cut-over to generator power can be accomplished.

14. Color-Coded Badge System

Segregate the data center into various control zones based on sensitivity (e.g., tape library, DASD area) and issue color-coded badges identifying the areas to which personnel are authorized access. These badges can be used in lieu of in conjunction with an electronic access control system. Develop procedures for issuing, controlling, and retrieving the badges.

15. Control of Chilled Water Supply

Ensure that:

- Pumps used for chilled water distribution are in a physically secure area.

- There is an alternative source of chilled water in the event that the primary source fails.
- Chilled water pipes are adequately insulated to prevent condensation build-up and leakage onto equipment.

16. **Secure Air Intake Ducts**
Ensure that unauthorized persons cannot enter the data center by crawling through air intake ducts, using alarmed tamperproof grates.

17. **Secure HVAC Equipment**
Install HVAC equipment in a physically secured location.

18. **Secure UPS and Motor Generator Equipment**
Ensure that UPS and motor generator equipment are in physically secured location.

19. **Secure Electrical Distribution Panel**
Ensure that the electrical distribution panel is in an area physically secure from access by unauthorized persons.

20. **Emergency Power Shut-Off**
Equip facility with an automatic power shut-off that will kill all electrical power to equipment upon activation of any smoke or heat detector in the facility. In addition, install manual shut-down switches at all fire exits.

21. **Floor Lifters**
Provide floor lifters wherever hand-held fire extinguishers are placed.

22. **Hand-Held Extinguishers**
Mount hand-held extinguishers (preferably Halon 1211) strategically in the equipment area in accordance with NFPA standards [4].

23. **Fire-Resistant/Noncombustible Furnishings**
Ensure that all curtains, carpeting, furniture, raised flooring, false ceilings, insulating material, and so on are made of noncombustible materials or are treated with fire-retardant materials.

24. **Waterproof Covers**
Equip the computer room with waterproof equipment covers to prevent damage from flooding or sprinkler discharge. Develop written procedures outlining the use of the covers and ensure that personnel are familiar with them.

25. **Water Detectors**
Install water detectors under raised flooring and around water chiller units and pipes.

26. Under-Flood Drainage
Provide adequate drains under raised flooring areas around water chiller units and pipes. Regularly inspect drains to make sure they are open and free of trash.

27. Watertight Ceilings
Ensure that ceilings are sealed and watertight to prevent damage from water leaking from higher floors.

28. Visitor Control
Treat all personnel not requiring regular access to the facility as visitors. Visitor-control procedures should include:

28.1 · Issuance of a distinctive badge that identifies the wearer as a visitor.

28.2 · Requiring all visitors to sign in and out of the facility on a visitor log. Logs should be checked at the end of each shift to ensure that all visitors are accounted for.

28.3 · Requiring visitors to be escorted at all times while in the facility.

29. Vendor Personnel Control
Control access by vendor personnel, such as customer engineers and maintenance technicians, by having them:

29.1 · Undergo the same background screening as other personnel with access to the same facilities and systems.

29.2 · Issued contractor badges. Replacement personnel sent by the vendor, however, should be treated as visitors until receipt of proper access authorization.

30. Backup-Media Security
Take adequate physical security measures to safeguard backup magnetic media (disks and tapes) during both transit to off-site storage and storage at the remote site. These measures include:

- Moving media to off-site storage in double-locked containers under dual control.
- Written procedures covering the authorization of personnel to perform the transfer.
- Continuous receipting at both the point of origin and the destination.
- Providing the same level of physical protection at the off-site location at the primary site.

31. Destruction of Sensitive Output
Provide adequate written procedures and equipment (e.g., degaussers, pulpers, paper shredders, incinerators) for the destruction of sensitive printouts, carbons, microfiche, and other human-readable media; and ensure that they are used.

32. Guard Force

Use a guard force (whether organizational personnel or a professional group) to provide 24-hour-a-day control of entry and egress to the facility in which the data center is housed, the date center area, equipment areas, and other areas of especially high sensitivity (e.g., tape library, DASD area).

33. Limit Entry/Egress Points

Permit all entry and egress to the data center, equipment areas, and media library only through a single point controlled by an electronic access control system, locking devices, and/or guard surveillance. This can be accomplished very efficiently by the use of a double door, with one door opening inward for entry, the other outward for egress.

34. Media Library Procedures

Establish a magnetic media library, and develop written procedures for library operation: a procedures manual for using any automated tape management system, a regular schedule of tape cleaning/maintenance, and procedures for movement of backup media to and from off-site storage (see also Countermeasure 30). A retention schedule for data stored on magnetic media, accountability for new media and the retirement of old media from active service, and an inventory of magnetic media should also be detailed. Although the size of the operation will determine the size, staffing, and organization of the library, certain minimum procedures should be followed in all cases:

- 34.1 · Lock all data and program files in a fire-resistant room or container when not actually in use. Access should be limited to authorized personnel only.
- 34.2 · Develop sign-in/sign-out procedures to account for all media.
- 34.3 · Have a media librarian present on all shifts. If only one librarian is employed or the function is performed by a member of the operations staff on a part-time basis, control access to media by dual custody of lock combination/keys.

35. DP Security Training

Establish a DP training program for all personnel, covering such areas as:

- · Organizational security policy--All employees should be aware of the organization's security policy and their responsibility to protect data and other resources from misuse, theft, or destruction.
- · Security operating procedures--Train employees in day-to-day procedures for handling sensitive data/programs, conducting security checks, and maintaining the security and integrity of systems and facilities.

- Access control procedures--Delineate the types and levels of access to facilities and systems, access control systems in use, and escort policy and procedures.
- Security incident procedures--Discuss the handling of bomb threats, riots/disturbances, unauthorized personnel in controlled areas, and emergency reporting and response.

36. Insurance

Purchase insurance to lessen the financial impact of physical loss, computer fraud, and malpractice. Among the types of coverage that should be considered are:

- Property Damage--Insurance can be obtained to cover the damage or destruction of facilities, systems, data, programs, and other tangible assets. Acceptable levels of loss retention should be established.
- Fidelity Coverage--Most organizations can obtain fidelity coverage to indemnify them against fraudulent acts (including computer fraud) by employees.
- Business interruption--In addition to property damage, the coverage should be sufficient to indemnify the organization for loss of revenues resulting from damage to or destruction of DP resources.
- Third-Party Penetration--New coverage indemnifies the organization against the penetration and manipulation of DP or communications systems for fraudulent purposes by persons not employed by the organization.
- Errors and Omissions--Coverage is available that insures against loses caused by errors and omissions on the part of employees and contractors.

37. Shock-Mounting Equipment

In areas of seismic activity, install disk drives and other vibration-sensitive equipment on free-floating shock mounts to minimize the vibration damage.

38. Balanced Circuits for Security Systems

All electrically activated security systems should operate on a balanced circuit designed to detect a ±10 percent change in line current, and thus prevent covert disablement of security systems by intruders.

39. Emergency Action Training

Establish an emergency action training program to ensure that all personnel are thoroughly familiar with their duties and responsibilities during emergencies. This training should be given to all employees within two weeks of

starting employment and refresher programs should be conducted on a regular basis. The training should include:

- Fire evacuation/suppression
- Bomb threats
- Natural disasters
- Terrorist activity
- Power outages/failures
- Emergency first aid, including CPR.

PERSONNEL SECURITY CONTROLS

40. Data Classification Standards

Develop data classification standards to determine which data processed or stored by automated systems requires additional protection beyond that normally provided. The sensitivity or criticality of data should be examined in three areas during a formal evaluation process:

- Proprietary--Data that provides the organization with an advantage over competitors or whose disclosure might expose the organization to fraud.
- Privacy--Data that is covered by current or anticipated privacy legislation or that should not be disclosed for legal or ethical reasons.
- Criticality--The importance of given data to the organization's operations (generally described as a function of how long the organization could afford to be without access to it).

Levels of classification (e.g., internal use only, company secret) should be developed; the degree of protection afforded data and the level of access allowed should be a function of this classification.

41. Position-Sensitivity Levels

Evaluate the sensitivity of DP positions within the organization to determine the permissable level of access to sensitive data as well as the depth of background checking that must accompany the hiring of an individual. The sensitivity of DP positions can generally be thought of in the following hierarchy:

- Extremely sensitive
  --DP auditor
  --Security officer
- Highly sensitive
  --Computer operator
  --Data entry operator
  --Operations manager
  --System programmer
- Sensitive
  --Computer system engineer
  --Programming manager
  --Application programmer

--Tape librarian
--Data administrator/data base manager
--Customer engineer/maintenance engineer
--Communications equipment maintenance technician

- Moderately sensitive
  --Physical security personnel
  --Peripheral equipment operators/maintenance technicians
  --I/O control/data control clerks

42. Background Checks

Conduct background checks for all personnel in sensitive DP positions, basing the thoroughness of the check on the level of job sensitivity:

- Level 1--Extremely/highly sensitive
  --Polygraph/psychological stress analysis (where legal; see also Countermeasures 51 and 52)
  --Background examination by investigative personnel
  --Credit check
  --Criminal record check
  --Education record check
  --Reference check
- Level 2--Sensitive
  --Background examination by investigative personnel
  --Credit check
  --Criminal record check
  --Educational record check
  --Reference check
- Level 3--Moderately sensitive
  --Credit check
  --Criminal record check
  --Reference check

43. Security Briefing/Nondisclosure Statement

Give all new personnel within the DP function a detailed security briefing before they start work. This briefing should describe the security aspects of the organization's operations and delineate organizational security procedures, including reporting of security incidents and general and specific security responsibilities. After briefing, all new employees should execute a nondisclosure statement certifying that:

- They have been informed of and understand their security responsibilities.
- They understand the disciplinary and legal penalties associated with unauthorized use of resources or disclosure of data.

44. Personnel Rotation

Rotate personnel involved in sensitive duties. Not only does rotation broaden the individual's knowledge of the operation and provide highly desirable cross-training for

purposes of backup, it also helps deter the possibility of fraud based on collusion. In addition, it serves to prevent individuals from becoming locked-in to a particular position by providing professional challenge and job stimulation. Persons in boring and/or repetitive jobs (data entry and data control, for example) should be rotated to ensure that they do not feel or become stagnant and to enhance morale. Personnel left in the same tedious job for long periods may become disgruntled or careless, resulting in willful or inadvertent errors and omissions.

45. Mandatory Leave of Absence

Require all personnel in sensitive areas to take a stipulated leave of absence (at least two consecutive weeks) each year. This allows pending transactions to clear and helps to identify and isolate potential fraud.

46. Proper Management and Supervision

The success or failure of any security program can be traced to employee attitudes toward both security and the organization itself. There is a clear correlation between employee dissatisfaction and the incidence of employee carelessness, theft, fraud, or other misconduct. Management should therefore address a number of issues, including:

- Work environment--Make sure that work spaces and conditions reflect management's concern for employee well-being and productivity (see Countermeasure 10). Provide adequate lighting, in terms of the number and type of units, proper dispersal and placement, and prompt replacement of burned-out or defective units. Noise suppression should include carpeting; acoustical tiles, baffles, paneling, and equipment covers. Provide adequate ventilation and proper temperature and humidity (see Countermeasure 11) and effective fire detection and suppression equipment (see Countermeasures 4 and 5). Exits should be appropriately marked and easily accessible.
- Professional Growth--Challenge and growth are major motivating factors for DP professionals (as well as for other employees). Encourage employees to participate in professional organizations and to continue their education, through both external training and in-house professional development seminars.
- Performance Evaluations--Use frequent informal performance evaluations to give employees feedback on job performance and to offer them a chance to express their feelings about the working environment and their own career progress. Evaluations can also uncover potential problem areas before they become serious.

- Personal incentives--Consider instituting security award programs to reward employees who report theft, fraud, or other unauthorized use or manipulation of DP resources; such programs can become part of the performance evaluation.
- Detection and deterrence--Organizations whose employees believe they are likely to be caught if they engage in unauthorized activities experience a significantly lower level of theft and fraud. The more severe the reaction of management and co-workers, the lower the number of incidents (co-worker sanctions are particularly effective).
- Grievance Procedures--Establish fair and equitable grievance procedures and administer them impartially. Management at all levels should be attentive to grievances and act promptly on those that are justified.
- Awareness of personal problems--Be alert to major changes in the personal as well as work habits of subordinates. Such changes frequently signal an increased potential for fraud, misuse of resources, or disclosure of sensitive data. Changes in attendance patterns, evidence of alcohol and/or drug abuse, an inordinately high standard of living in relation to salary, severe indebtedness, and similar changes may indicate serious personal problems. Managers should investigate the causes of these problems and use all available organizational mechanisms to provide effective and timely assistance.

47. Termination Procedures

Upon notification to or by the employee of an intention to terminate employment, the supervisor should immediately:

- Notify the DP security officer and the personnel department of the pending termination.
- Request cancellation of all passwords/user IDs to which the employee has access, and have the employee turn in all keys, documentation, manuals, and other organizational material in his or her possession.
- Relieve the employee of all responsibilities involving sensitive data or programs and provide nonsensitive work instead. If nonsensitive work is unavailable, the employee should be relieved of all duties. Further access by the employee to the premises should be as a visitor and controlled as such.

The DP security officer should immediately:

- Cancel all passwords/user IDs pertaining to the employee.

- Change cryptographic keys or authentication codes to which the employee has had access.
- Brief the employee on his or her continuing legal responsibility to protect sensitive proprietary data after termination of employment. Have the employee execute a security termination/nondisclosure statement signifying his or her understanding of these responsibilities.

48. Formal Position Description

Develop formal position descriptions that incorporate levels of sensitivity and the need to restrict access to data and programs; describe the scope, content, and specific duties of each position. The descriptions provide personnel with a clear delineation of their duties; they also provide the organization with a standard against which individual performance can be measured.

49. Separation of Duties

Use the two-man principle by involving several people in the performance of sensitive duties. Such separation makes fraud more difficult by increasing the number of individuals who must be party to the fraud, and it provides an important error-checking and quality-control function. Separation of duties restricts the DP-related activities of the following groups of employees:

- Programmers:
  --Programmers may not both specify and write a procedure.
  --Programmers may not write and test the same procedure.
  --Programmers may not develop and maintain the same procedure.
  --Programmers may not write a procedure and maintain that procedure in the program library.
  --Programmers may not write a procedure and then execute it in a production mode.
  --Programmers may not control any transfers between programmer development libraries and production libraries.
- Operators:
  --Operators may not make changes to application or system software.
  --Operators may not have access to source code or source listings. Access to all other documentation should be on a strict need-to-know basis as required for actual processing.
  --Operators may perform no balancing activities except those necessary for run-to-run controls.
  --Operators may execute only programs scheduled through the established proper procedures.

--Operators may not execute data or software-modifying system utilities (e.g., IBM's SUPERZAP) without proper authorization and dual control.
--Operators may not execute programs from text libraries during production runs.
--Operators may not override internal labels without supervisory approval.

- Users:
--Data entry personnel may not prepare source documents for input.
--Someone other than the input operator must verify all data input, unless programmatically verified.
--The same person may not perform input and output duties.
--The same person may not post and balance general ledger and other sensitive entries.
--The person who prepared the original transaction may not prepare rejects or nonreads for reentry.
--Master file and other sensitive transaction changes must be under dual control.

50. Preemployment Suitability Testing

Use preemployment suitability testing. These tests, which can be quickly and easily given to applicants, do not violate the legal prohibitions present in many states on the use of polygraphs or psychological stress analyzers in preemployment screening (see Countermeasures 51 and 52). Field experience has shown that a high percentage of applicants who fail these tests have a history of theft, drug or alcohol abuse, or emotional instability.

51. Psychological Stress Evaluation (PSE)

PSE equipment measures the level of stress present in a subject's voice. Measuring this stress level is said to enable determination of whether an applicant is answering questions truthfully in preemployment interviewing. Use of this technique, however, has raised legal and ethical questions, and some states have outlawed such testing.

52. Polygraphic Examination

Polygraphs measure the electrical conductivity of the skin. They have been used during the past 20 years to give some indication of the truthfulness of answers to questions posed during an interview. Serious questions have been raised regarding their accuracy, however, and many states have outlawed them for preemployment screening.

53. Power Filters
In installations that do not use conditional power, equip all DP hardware with power filters to prevent damage to hardware or data from power surges and spikes.

54. Minicomputer-Based Hardware Monitors
Use minicomputer-based hardware monitors for the collection and analysis of large quantities of data in real time without placing excessive overhead on the operating system. Security personnel can thus constantly monitor and analyze system activity without degrading the speed and quality of processing. Use of an independent security monitor also makes the system far less vulnerable to subversion and unauthorized access, since would-be penetrator must avoid both the security safeguards of the mainframe and the surveillance of the external monitor. Illegal requests or those inconsistent with the terminal's authority, excessive log-on failures, and attempts to use deactivated but still resident software should be monitored and logged.

55. Hardware-Generated CPU Identification Code
The system uses a hardware-generated code that identifies a particular CPU (especially useful in networks of multiple CPUs).

56. Program-Readable Clock
This system uses a clock word in memory that can be read (but not written) by user programs; it is essential for logging, since it gives the capability of affixing a time stamp to a message or transaction.

57. Ring Architecture
In this form of system architecture, data and/or programs are organized into a fixed number of hierarchically ordered rings. The higher the number of the ring, the lower the level of privilege; ring zero is the highest level of privilege. User programs executing within a given ring are then granted access to segments in rings at their own or a lower level of privilege (i.e., a higher-numbered ring), protecting segments in lower-numbered rings. Illegal instructions should cause an interrupt.

58. Capability-Based Architecture
This architecture requires that each program maintain a table of absolute addresses of all segments it has the authority to access. A program is then said to have the capability of accessing these segments. When a program requests a segment, the executive checks its access privileges; if access is authorized, the program is given the access capability for that segment.

59. Prohibition of Unspecified Operation Codes
The system recognizes all allowable operation codes; those unspecified are denied execution.

60. Memory-Clearing Instructions
An operating system function is used to overwrite with zeros all areas of core memory and/or mass storage used by a program, after program execution and before releasing storage for reuse.

61. Segmentation
This scheme, in which the architecture supports segmentation, is similar to paging except that variable-length blocks of memory are used. Thus, a program can define logical blocks of memory (modules) to constitute segments. This decreases the frequency of swapping, since once a module is brought into main memory, it usually remains there until it finishes execution and exits. Segment tables store the origin and length of each segment, permitting the sharing of segments between multiple users. These tables also control user access to shared resources.

62. Paging
Mass storage is subdivided by hardware/software into pages of equal size; these are then used as an extension of main memory. Memory mapping using resident tables and hardware registers is then performed to map the program's virtual memory space with its physical location, which will generally be divided between main memory and mass storage. A page fault occurs when a program attempts to fetch or store data not resident in main memory. The page containing the desired virtual address is located and its contents swapped into main memory.

63. Storage Locks and Keys
The architecture uses bit masks to protect specific blocks of main memory, and the operating system places a lock at the beginning of each such block of storage. Each operating program (including the executive) has a key that is kept in a hardware register. Each program is authorized access only to those blocks whose locks match this key. The executive is assigned a key of zero that accesses the locks of all other operating programs.

64. Memory-Bounds Registers
Memory-bounds registers consist of a base-address register and an upper-limit register that are loaded by the operating system when a job is brought into main memory. Each memory reference by the job is checked to ensure that it neither exceeds the memory allocated to it nor intrudes on memory locations allocated to other jobs. There should be an attribute register for each bounds register. These

registers contain values that indicate the type and characteristics of the data being stored and protected; they allow implementation of more complex protection mechanisms (e.g., read only, write only) in the hardware.

65. Firmware Implementation of Sensitive Functions
Because of the recognized subvertability of software, certain critical functions (e.g., access control tables, sensitive operating system routines) can now be firmware based (burned into chips). Execution speeds can be dramatically increased, and security is enhanced because of the difficulty of covert firmware modification. Physical access to firmware, nevertheless, should be limited and strictly controlled and monitored. Install locks and counters that show how many times the cabinet has been opened on all cabinets containing firmware. Regularly inspect all firmware components for signs of tampering.

66. EMI Containment Procedures
Use electromagnetic interference (EMI) containment procedures to minimize the possibility of compromising emanations being intercepted. These measures include:

- Use of TEMPEST-approved equipment[1]
- Use of EMI shielding material to insulate the room or the equipment housing.
- Use of internal EMI suppressors on equipment.

67. Physical Control Zone (PCZ)
Establish a PCZ to control EMI and to prevent unauthorized personnel from entering it to monitor electronic emanations. The zone should be large enough so that, at its perimeter, the level of signal strength that can be acquired is less than 10 microvolts per square meter.

SOFTWARE SECURITY CONTROLS

68. Life Cycle Approach to Software Development
Use of a life-cycle approach improves management's view of and control over the software development process. This methodology defines the various phases of software development, implementation, and enhancement, all of which affect the security of the system, dividing these phases into major milestones and activities. The major phases in the life cycle of a software system are:

- Initiation and survey--The goals and benefits of the project are described and the actual need for the system determined.

---

[1]TEMPEST refers to a government program involving the building of components that effectively contain emanations.

- Functional requirements definition--Major user needs and processing requirements are defined.
- System architecture definition--Various alternative methods of addressing the functional requirements are identified and defined.
- User design--The external design of the system (i.e., how it will appear to the user) is defined, as are all processing and I/O requirements and the like.
- System design--High-level user requirements are translated into specific system requirements, such as file structure, data base, I/O, data capture, security and control, and testing.
- Implementation--All designs and plans from the previous phases are translated into executable programs that perform in the test environment according to specification. The entire system is run through acceptance testing. The system is then installed as part of the production environment.
- Maintenance--The objective here is to ensure that each production application performs in an optimum manner as perceived by users, computer operations, and systems development.

69. Software Development Methodology

Formulate and publish a formal set of software development standards within the organization. This publication should take the form of a systems programming and standards manual applicable to all organizational elements.

Use a structured methodology such as top-down development, which consists of the following phases:

- Top-down design--Software should be designed so that it identifies first the major functions to be accomplished, then the lower functions derived from these. A tree structure is designed, containing these subfunctions with the highest level of control logic in the top segment and control passing to lower-level segments. This process continues for as many levels as required until all subfunctions are included in the structure.
- Top-down implementation--Implementation of the design produces a top-down hierarchy of subfunctions. No program component is generated until the component upon which it depends has been produced.
- Top-down testing--The highest-level segment is tested once it is coded; this segment then exits to the next-lower segment, which is also tested (if it has been coded). Since higher-level segments are used to exercise lower-level segments, careful design and planning will ensure that the most critical subfunctions are also the most tested.

70. Documentation

Document systems adequately throughout their life cycle so that all system and program functions are recorded for use in subsequent design efforts and for support of system audits. Documents produced during the development or enhancement of a system and/or program should include:

- Functional description--Prepared during the definition stage of the system life cycle, this offers a high-level definition of the functions to be provided by the operational system. Since the functional description is used by both technical and nontechnical personnel, it should contain a minimum of computerese.
- Data requirements document--This is a technical document prepared by both development and user personnel, providing as much detail as possible in the following areas:
  --Input required
  --Procedures for providing input to the system
  --Expected output
  --All uses of standard data elements
  --Data limitations of the system
- System/subsystem specification--This technical document is prepared during the design phase to guide system personnel during the development of large projects. It provides more detail concerning the system environment and design elements than does the functional description. System/subsystem interfaces are also defined.
- Program specification--Used to guide program development during detailed design, this provides more detailed data requirements than either the functional description or the system/subsystem specification. The program specification is concerned with only the segments of the description and specification that can be applied to a particular program.
- Data base specifications--These documents are prepared for use when many analysts/programmers are involved in writing programs using the same data. The specifications must be detailed enough to allow program coding and data base generation by the development team.
- User manual--Directed to the system user group, the manual provides the following guidance:
  --General and/or specific information on a given computer system or program, oriented toward general management and staff personnel
  --Details on providing system input
  --Responses required to system requests
  --System output procedures and formats
  --Instructions for operating peripherals

- Computer operations manual--This is directed toward supervisory and control personnel, providing the detailed operating procedures necessary to initiate, run, and terminate the system.
- Program maintenance manual--This manual provides general and specific information about the computer program for maintenance personnel, offering detailed technical presentations of computer programs.
- Test plan--This provides a mechanism for directing a comprehensive system testing program, enumerating test events, schedules, and materials.
- Test analysis report--This describes the methodology and results of system/program testing.

Establish a master documentation library, with written procedures to ensure that all documentation contained in it is current. Control access to the library on a strict need-to-know basis.

71. Software Quality Assurance

Establish a formal software quality assurance group within the data processing organization. This group's charter should stipulate that it reviews all software and related documents for:

- Accuracy, consistency, and readability
- Conformance to security and control standards
- Conformance to system and program specifications
- Adequacy of documentation
- JCL and other control errors that might create problems in a production environment

All software products and related documentation should constitute a reliable and maintainable product.

Conduct a software quality assurance review when:

- A major change is made to any production system
- Any change is made to a critical or sensitive system
- Any software product from a third-party vendor is delivered
- A new system development effort is completed

Ensure that all test kits (test programs designed to exercise specific application software systems) are maintained by quality assurance. Changes to these kits should be performed by quality assurance with input from the systems development staff.

72. Configuration Management (CM)

Use this technique to control the evolution of the modifications to a system during its development. Technical and administrative direction and surveillance should be applied to identify and document the functional and physical characteristics of hardware and software. CM also controls

changes to these characteristics and records and reports change processing and implementation status, minimizing the possibility of unauthorized hardware or software modification.

73. **Verification and Validation (V&V)**
Use software V&V to ascertain that system requirements are accurately stated, that the software is being developed in accordance with the stated specifications, and that in operation it satisfactorily performs the functions for which it was designed.

- Verification--This substantiates that requirements, design, and code are complete and consistent with each other. It involves the review of all software life cycle to ensure that they conform to earlier documents and will ultimately conform to the requirements.
- Validation--This confirms the feasibility and testability of requirements and the correctness of the design and code. It involves exercising and analyzing the software to ensure its performance according to specifications and to discover latent errors. Validation provides greater guarantees of a correct system by comparing expected results with actual system performance when the system is extensively exercised.

74. **Chief Programmer Team Concept**
Use chief programmer teams to break a large system production group into smaller groups to minimize problems and errors. A programming team consists of a leader and usually fewer than eight members. The team is given complete responsibility for a portion of the system and is expected to produce well-implemented well-defined software for that portion. Keeping the group small minimizes problems, especially those of communication.

75. **Structured Walkthroughs**
Use this technique, in which the designer/author simulates the execution of the program/system segment in front of a peer group for their evaluation, to review the logic and functionality of system and program design prior to actual testing of code modules. Such reviews are informal and are usually completed within one or two hours.

76. Program Librarian
Use an operating system containing a program librarian to provide maintenance of software programs within the system. The library consists primarily of internal and external entities. The internal library is maintained in a disk file and contains the programs and job control statements that have been generated by the programming team. The external

library consists of program source listings, test results, and the like. The librarian function adds, deletes, and modifies library programs and maintains a record of library program accesses for use as an audit and surveillance tool. In an automated environment, interface the library management system with access control software to provide data set protection for library accesses.

77. Software Documentation Reviews

A software documentation review is an audit and validation of developed software. Based mainly on the source listings and any available system documentation, the review and audit are directed primarily toward software development improvements. The process should increase confidence in the software and produce a more reliable and maintainable product. Software documentation review activities fall into the following four areas:

- Familiarization with and review of the code and applicable documentation
- Review of software construction and coding techniques
- Generation of a functional description based on derived functional requirements and knowledge of the software
- Analysis of the functional description and its relationship to the actual implementation.

78. High-Order Languages (HOLs)

Use a high-order language that provides control structure and/or data structure features, allowing programming to be done at the abstract and machine-independent level. Such programming takes less time and produces more readable, auditable, and maintainable code than does assembly language. HOLs include FORTRAN, COBOL, ALGOL, PL/1, Pascal, CMS2, and Ada.

79. Access Control Software

Use access control software (e.g., RACF, ACF2, SECURE, SAC, TOP SECRET) for enhanced control of access to sensitive data.

80. Internal Tape Labels

Use a tape management system that assigns magnetically encoded labels and does not rely on external serial numbers on tape reels. This greatly reduces the possibility of inadvertently or willfully mounting and running unauthorized tapes or altering external labels.

81. Data File Encryption

Provide a high level of security to stored sensitive data by means of file encryption. In this process, data is encrypted prior to its storage on magnetic media. Theft of

the medium or unauthorized file access will yield only data in encrypted form. Authorized users, however, can decrypt the data at the time of file opening. Unlike link encryption (see Countermeasure 114), file encryption is software rather than hardware based. If a system based on the data encryption standard (DES) is used, ensure that keys are stored in encrypted form and changed regularly.

82. **Automated Code Analysis**
Use automated code analysis to validate code in relation to its specification. This tool is also effective in reviewing and evaluating software construction and coding techniques with respect to accepted industry standards and practices. It can be used to facilitate certification of newly developed security-related software and to provide fast and accurate auditing of existing programs to detect unauthorized code modification.

83. **Self-Metric Software**
Use a software routine that contains embedded code to meter the performance of specific activities, for example, the amount of main storage or other system resources accumulated by the routine's associated processes.

84. **Trace Program**
Using a trace program to aid in error detection. This diagnostic tool is an operating system capability that provides a sequential record and analysis of each instruction executed in a program. If files are created, they should be deleted after program execution. The trace programs should display the values of variables and program instructions; they should not change the value of any variable, instruction, or data, nor should they alter the course of execution. In some cases, the use of trace programs might itself be considered a threat, and adequate controls protective must be placed on all sensitive files that might be accessed by the trace program(s).

85. **Time-Out Feature**
Ensure that the operating system provides the timing services required to support a secure operational environment. Both time-of-day clock and CPU (interval) timer facilities should be supported. Task management should use timer services to control and limit CPU use through scheduling algorithms. Inactive processes, or terminals (in an interactive environment) should be terminated after a predetermined period.

86. **Threat Monitoring**
Ensure that the operating system provides threat-monitoring information. The system should record data on the following events as often as the user desires:

- Unauthorized attempts to enter the system
- All attempts (authorized or unauthorized) to access protected resources
- All attempts to issue restricted commands
- All attempts to modify profiles on restricted data

The system should route messages to the security console, and each incident should be recorded on the security log/audit trail.

87. Security Auditing and Accounting

The system security auditing and accounting capability should, as a minimum:

- Record all unsuccessful log-on attempts to the system
- Record all attempts to enter supervisor mode
- Record all attempts to access restricted schemas/subschemas
- Record all trapped requests requiring extended access authorization
- Log all system transactions, including jobs on/off, with user/terminal/program ID and the date time group (DTG)
- Log data/files requested and/or accessed, including access keys and the number and types of access
- Log the disposition of data, including number of records input/output/displayed and terminals or logical devices to which data is output.
- Log crashes, machine failures, and restarts
- Log program aborts
- Log changes to security access tables
- Log program library updates
- Log all descriptor changes.

88. Security Labeling

Ensure that the system labels all input/output with security and/or sensitivity labels and checks routing indicators before data output. Data objects should be labeled with security information, and the operating system should check all labels before processing.

89. Extended Access Checking

Ensure that the system has the capability for an extended method of access authorization such as an extended handshake or question and answer (see Countermeasure 117) to restrict access to data or processes. The software that controls the handshaking must require proper data and must log all access attempts.

90. Operating System Identification of Terminals

All terminal activity should be controlled by the operating system, which should be able to identify terminals, whether they are hardwired or connected through communications

lines. A chart should be created for use in identifying and locating terminals according to their IDs.
The operating system should inspect log-on requests to determine which application the terminal user desires. The user should identify an existing application and supply a valid user ID and password combination (see Countermeasure 119). If the log-on request is valid, the operating system should make a logical connection between the user and the application.

91. Operating System Control of Data Transfer
Maintain positive control of all data transfers between files and logical devices through the operating system. Performing error and parity checking on each fetch and transfer cycle prevents the injection of malicious or inadvertent errors into the system during data transfer.

92. Operating System Control of Resource Allocation
The operating system dispatcher should control processor allocation, using a priority queue determined by the users and the installation's established policy. As each task is dispatched, a control register should be loaded with the address of the task's unique address translation table. The control register should not be accessible by the user program, and the tables should be retained in storage areas that are not among the user program's read/write/execute capabilities.

93. Operating System Control of Maintenance Software
The operating system should permit access/execution of utility software only in the system state or privileged mode. This feature protects against covert modification of software. Special care should take in the control of utilities such as SUPERZAP, with all accesses and/or uses logged and reported.

94. Operating System Control of Executive Mode Access/Execution
The operating system should have the capability to create two modes or states for processor operation: supervisor and user states, which operate in privileged and unprivileged modes, respectively. Certain processor instructions are designated privileged and can be executed only when the processor is operating in the privileged state. Privileged instructions, for example, are those that:

- Perform input/output
- Control the interrupt mechanism
- Set base and bounds registers or locks and keys

User programs execute with the processor in unprivileged mode, and any attempt to execute a privileged instruction is trapped by the processor.

95. Operating System Erasure/Purge of Residual Data
The operating system should have the capability (by overwrite, dump restore, or the like) to erase or purge residual data. This should be performed on all main memory locations and peripheral storage after completion of classified or sensitive processing and before reallocation of system resources to another user.

96. Virtual Machine Monitor (VMM)
The VMM, the central control program in a virtual machine system, supports an extended machine on which user programs can be run. Since the VMM can support programs that use the full capability of a computer system, it can support complete operating systems in the same way that operating systems support user programs. Therefore, it is possible to run two incompatible operating systems on a single computer at the same time or to run one operating system in production mode while system programmers simultaneously modify another active copy of that operating system. The VMM effectively operates as an isolation mechanism.

97. Job Management
The principal job management functions of the operating system should be provided by a job entry subsystem, through which all jobs, started tasks, and time-sharing log-on requests should enter the system. The job management function performs the following basic tasks:

- Reading jobs into the system
- Scheduling jobs for execution
- Maintaining all data submitted with jobs
- Supporting the system management facilities
- Handling output from jobs and time-sharing users

98. Job Scheduling
The operating system should provide job scheduling functions consistent with a secure processing environment. Input an output data streams should be handled in a manner that restricts access to the associated job through the use of dynamically allocated spool space (see Countermeasure 99).

99. Job Spooling
The operating system should provide the spooling function for input and output data streams. It should follow naming conventions for spooled data sets that guarantee restricted access (e.g., input data sets can be accessed only b the job that created them). Similarly, spooled output should automatically be associated with the creating job.

100. Interrupt Handlers
Operating system interrupt-handling programs should support hardware features that supplement the security feature of the task management functions. In addition to detecting

external signals for service and normal completion of I/O requests, the interrupt mechanism should recognize the following potential security violations:

- Attempts to execute undefined instruction code
- Attempts by programs executing in user (unprivileged) mode to execute privileged instructions
- Attempts to reference unallocated storage addresses
- Attempts to exceed current capabilities when referencing allocated storage (e.g., attempts to write in read-only areas)
- Attempts to reference main storage allocated to other user jobs or any of the various operating system functions
- Attempts to issue invalid commands to storage devices

After the attempted operation has been aborted by the hardware, the interrupt handler should routinely terminate the user program.

101. Recovery Management

Recovery management facilities should handle error processing for both hardware and software failures, so that system processing can continue with minimal downtime.

- Software failure recovery--The recovery facility should monitor the flow of software recovery processing by handling all abnormal terminations of tasks and address spaces and passing control to recovery routines associated with the terminating functions.
- Hardware failure recovery--The operating system should have the capability to gather information about hardware reliability and allow the user to retry operations that failed because of processor, I/O device, or channel errors. This feature should be designed to keep the system operational in the event of hardware failures.

102. Indirect Addressing

All addresses passed between the system and the user should be logical in nature rather than real, protecting memory address locations of classified or sensitive data.

103. Paging

The paging supervision routines of the operating system should be responsible for transferring individual page contents and swapping complete user page sets between main and secondary storage. Tables that provide a directory to the contents of each available page on the direct-access data sets should be accessible only by executive-mode routines.

104. Data Base Access Controls

Data base access controls should be provided at the user, data, and process levels. Loggings of all accesses and attempted accesses should be available, and the DBMS should provide concurrent access controls and deadlock resolution.

105. Data Dictionary Controls

Certain data dictionary features enhance security in the data base; these features include:

- Level of integration--A highly integrated data dictionary requires greater security measures. Develop procedures to prevent misuse of the additional capabilities integration offers.
- Access control--The data dictionary should have access controls to prevent any unauthorized use or modification.
- Backup--Establish procedures for keeping a current certified copy of the data dictionary.
- Certification/verifiability--Establish procedures for certification and verification of backup as well as production copies of the data dictionary.
- Program registration--The data dictionary should have a program registration capability to prevent unauthorized access or use.

106. Data Base Recovery

Provide the capability for rapid and efficient data base recovery, including:

- Backup--Utilities, programs, and procedures should be available to provide backup for the data base.
- Up-to-date copies--Current copies of all essential program files and the like should be kept available and secure.
- Documentation--Recovery and backup procedure documentation should be kept current.
- Levels of recovery--Provisions for selective recovery and definitions of acceptable degradation of service should be specified.

107. Data Base Maintenance

Adequate facilities and procedures for data base maintenance are essential for data base security. These include:

- Vendor interface--Vendor maintenance procedures should be established to ensure that security is not compromised.
- Ease of maintenance--Easy-to-maintain modules and well-defined software maintenance procedures are essential: lack of proper maintenance can cause security breaches.
- Maintenance responsibility--Clearly define maintenance responsibility and specify procedures for certification and verification.

- Evaluation/certification--Establish requirements for the evaluation and certification of the DBMS, and keep a certified audit copy as backup. Documentation relating to the DBMS should be kept current with the operational version.

COMMUNICATIONS SECURITY CONTROLS

108. Limitation of Log-on Attempts

Limit system log-on attempts from remote terminal devices. More than two unsuccessful attempts should result in termination of the session, generation of an audit entry and/or operator message, and purging of the input queue of messages from that terminal.

109. Passwords

Use passwords that require the user to enter a string of characters that are checked by the system against a system-resident password file. Access is granted or denied accordingly. Current password schemes include:

- Simple or fixed passwords--In this scheme, the user selects a fixed-length character string and stores it in the file prior to use. This system is inexpensive, it uses an easy-to-remember password, and it remains valid until changed by the user. However, user-generated passwords are frequently obvious (e.g., user's name, spouse's name) and are thus easily penetrated.
- Changeable (one-time) passwords--This scheme increases the integrity of a simple password by providing the user with a given list of passwords. The same list is stored in the computer in encrypted form. The user selects the first password on the list, which matches the first password stored on the system-resident table. The user then crosses that password off the list. Similarly, the system will not honor that password for subsequent requests, whether or not the user is authorized. Changeable passwords can also be used to authenticate the computer's log-off acknowledgement as well as the user's logoff request.
- Random passwords--In this technique, the user is supplied with a pseudo-random number at log-on, and transforms it algebraically, using a transform previously provided by the system. The system performs the same transformation instantly and compares the answers. Although a hostile individual may intercept the argument of the function or the answer transmitted to the computer, he or she does not know the nature of the transformation and its thus denied access to the system.

- Functional passwords--Multilevel protection codes stored within each user's password determine the user's level of access to specified processor functions and data sets.

110. Terminal Password Suppression
Use a nonprinting, password-suppression feature on all terminals to prevent the display of a user ID or password at log-on.

111. Process Lockout
Develop controls to restrict critical transactions to specific time periods such as normal working hours and prohibit their generation at any other time. Terminals used to process restricted transactions and critical files can be locked out physically and/or through system software controls (see also Countermeasures 85 and 116).

112. Control of Dial-up Mode
Use the following controls for dial-up networks:

- Maintain the confidentiality of dial-up telephone numbers and change them at regular intervals.
- Use automatic dial-back for caller authentication.

113. Restricted Dial-up Access
Restrict access of dial-up terminals to particular port(s) or front-end communications processors by equipping dial-up terminals with an identification chip that will generate a hardware identifier signal. This signal allows the communications processor to recognize the terminal as a dial-up and to route its messages to the designated port or processor (see also Countermeasure 124).

114. Communications Link Encryption
Use cryptographic devices to encrypt sensitive data transmissions. At the receiving end, a compatible device decrypts the communication. Monitoring encrypted communications thus yields an interloper only unintelligible text. Encryption also provides an additional source of message error checking, since any error occurring during transmission results in a change in the bit structure, causing the message to fail decryption.

115. Security Network Front Ends (NFE)
Using a minicomputer as an NFE provides surveillance and auditability between nodes in a network as well as protection between terminals and host processors at the nodes. The NFE can perform the same type of monitoring functions at the network level as those that are performed by the hardward monitor at the system level (e.g., transaction logging, access validation, surveillance, audit trail). This monitoring can provide a real-time profile of network use

and performance, permitting identification and isolation of problems before a serious compromise occurs. The NFE operates mostly logically, either as a component of the network control/management system or co-located with it in the network control center.

116. Hardware Terminal Locking
In areas that are not physically secured, equip terminals with locking devices to prevent their use during unattended periods. The locks should be installed in addition to programmed restrictions, such as automatic disconnect after a given period of inactivity (see also Countermeasures 85 and 111).

117. Dialogue Techniques
These are challenge/response techniques between the user and the system, such as:

- Extended handshake--To gain admittance to the system, the user must first satisfy a sequential decision procedure based on user-specific input parameters (e.g., user ID, password). This mechanism can restrict a terminal or user to certain physical locations, time periods, data sets, functions, or other attributes.
- Question and answer--This technique is based on system-resident tables of standard and user-supplied questions and answers. When a user attempts to log-on, some or all of these questions, chosen at random, are asked by the operating system. The user must answer all the questions correctly in order to be granted access.

118. Fiber Optic Cable
Use fiber optic cable to prevent physical wiretapping. Because fiber optics use light as the transmission medium, any break in the integrity of the cable (such as that created by a wiretap) will destroy the cable's conductivity, rendering monitoring impossible.

119. Shielded Cable
Use cable (e.g., coaxial cable) shielded to prevent electromagnetic radiation and designed so that any attempt to tap will result in destruction of the circuit and/or activation of alarm sensors.

120. Message Authentication Standard
Use the ANSIX9.E8 Message Authentication Standard[6] to authenticate messages, detect attempts at message modification, and increase the effectiveness of communications error checking.

121. Error Checking

Use polynomial error checking to detect errors in message blocks. This method uses a mathematical algorithm to check the structure and composition of bits transmitted against bits received: All the one bits in a message block are counted and divided by a prime number. The remainder (of this division) is transmitted with the message; the receiver performs the same calculation and matches the remainders. If the remainders match, the message has been received as sent. Attempts to tamper with the message as well as accidental changes caused by line noise and other nonmalicious factors can be detected.

All errors should generate an error message at the receiving end; each message should be accompanied by a description of corrective action to be taken by the operator. An explanation of all error messages should be contained in a user manual to be available at the network control center (NCC).

122. Message Parity Checking

Use both vertical and horizontal parity checking on all incoming messages. This is particularly important in asynchronous communications (e.g., TTY), since no time base common to sender and receiver is present (as it is in synchronous transmission). An 8th bit is added to the 7-bit ASCII coding structure. This bit, based solely on the value of the other 7 bits, is used to detect any change in the message during transmission. The technique is extremely useful in detecting both inadvertent and malicious changes in message content and structure.

123. Physical Security of Communications Appearances

Provide adequate physical security for all communications appearances (e.g., telephone cable rooms, cable runs) where physical wiretapping is possible. Measures to be taken include:

- Enclosure of all communications appearances in areas that can be locked and physically secured.
- Installation of cipher locks or magnetic key card devices on doors leading to wiring rooms or closets.
- Installation of magnetic contact alarms and motion detectors in areas that are not subject to 24-hour human surveillance.

Provide all modems, multiplexors, and patch panels with adequate physical security, including:

- Limitation of access to authorized personnel only
- Placement of modems, multiplexors, and other equipment in areas such as the network control center where they can be under 20-hour surveillance

- In remote equipment areas, CCTV coverage and installation of electronic intrusion detection systems

See also Countermeasures 1, 2, and 12.

124. Hardware Terminal Identifier
Fit all terminals using dedicated lines with a hardware identifier chip that so identifies the terminal to the system. This will allow controls to be developed to restrict access by user function and data as well as message origin (see also Countermeasure 113).

125. ACK/NAK
Use ACK/NAK for all messages. These characters indicate that the previous transmission was successfully received (ACK). If no previous message has been received, whether lost in transmission or simply not sent, the characters indicate a negative acknowledgement (NAK)>

126. Safe Storage of Messages
Safe-store all incoming/outgoing message traffic to protect against power or equipment failure or power surges or spikes.

127. Dynamic Polling Reconfiguration
Use dynamic reconfiguration of polling lists to restrict access by certain terminals during certain periods (see also Countermeasures 85, 111, and 116).

128. Automatic Answering/Automatic Outdialing
Use programmable front ends, concentrators, or modems for automatic call handling to increase efficiency and throughput.

129. Pseudo-Duplex/Full-Duplex Operation
Use a pseudo-duplex (which appears like a four-wire circuit) or a two-wire multiplexed circuit to maintain continuous carrier wave and increase transmission efficiency and reliability.

130. Line Backup
Have an automatic or manual dial-up line capability as backup for dedicated lines. Such facilities should allow outdialing only.

131. Modems with Automatic Equalization
Use modems with automatic equalization and balancing to compensate for line distortion, thus reducing line error and decreasing the need for conditioned lines.

132. Network Controllers/Network Management Systems

Eliminate the need for remote site test personnel by using automated remote monitoring systems that provide a central operator with all pertinent network status information. These systems, which can supervise large multiple-point and distributed processing networks, are designed around a master controller at the network control center. The controller is connected to special modules in each modem in the network that monitor the performance of their associated modems, collect status data, and respond to commands from the central controller. The central-site operator diagnoses faults in the network and initiates corrective action. Some of these systems are also equipped with a network management capability that provides statistical and trend reporting on network operation.

Such reporting is particularly important when:

- Central controllers change the polling configuration or in some way alter the manner in which terminals access the network, especially if:
  --The controller alters the time during which terminal(s) are granted access.
  --The controller alters rules that mediate the access of certain terminals or groups of terminals to the various processors, programs, or data accessed by the network.
- The central controller is used to establish both virtual and physical links between processor nodes in the network; that is, it establishes a circuit between one host processor and a terminal user of another host processor in the network.

133. Modems and Automatic Redialing

Use modems with automatic redialing capability to minimize downtime from line dropout. These modems should be available at the host processor only. Providing automatic redialing at a remote dial-up node might allow an interloper to cause a line dropout, followed by redialing of the host processor. Since the host would simply be reestablishing an existing connection, the safety feature of outdialing would not be used.

134. Multispeed Modems

Use modems with a multispeed capability (generally 300 to 9,600 bits per second). Lower speeds can be used when line error rates are high or when a larger number of slower circuits is desired, such as for online data entry or terminal inquiry. Higher speeds can then be used when line error rates are low and higher-speed transmission is more efficient, such as for bulk data transfer.

135. **Packet-Switched Networks**
Use packet-switched networks for both security and reliability. These networks divide all messages into packets and route them over different communications paths. This technique provides a higher level of reliability and makes message interception significantly more difficult.

136. **Communications Hardware Backup**
Maintain hot spares for critical communications hardware:

- Modems
- Multiplexors
- Cryptographic devices
- Digital switches
- Communications controllers
- Terminals
- Cluster controllers

137. **Digital Radio Backup**
In the event of total communication failure, patch slow-speed digital output through HF/VHF/UHF radio links.

138. **Communications Software Backup**
Maintain up-to-date backup copies of all communications software for use in the event of destruction or failure of the primary system. Storage should be on a secure off-site location.

PROCEDURAL SECURITY CONTROLS

139. **Review Access and Transaction Authority**
Establish a program for the regular review of user access privilege and transaction authority. Ensure that the authorizations are still necessary for user function and are restricted to the smallest number of people consistent with operational effectiveness.

140. **Verification of Transaction Authorization**
Establish a control function to verify independently the authorization of transactions before giving transaction documents to terminal operators for data input by having a verification clerk check the signature or query the authorizer by phone.

141. **Input Format Aids**
Use such input format aids as menus and data input masks to speed data entry and reduce operator input error, especially for financial and other sensitive transactions.

142. **Output Report Identification**
Ensure that all reports (including microform) contain the following identification information:

- Report date
- Report title
- User name
- Sensitivity level of report
- Disposal and control procedures (e.g., return to document control for destruction).

143. Suspended-Item Reconciliation
Ensure that all suspended transactions such as input errors are reconciled, either manually or through the program, at the end of each processing day or cycle.

144. Batch-Size Control
Limit size of input batches (e.g., no more than 50 source documents) for maximum control and facilitated reconciliation and batch verification.

145. Cross-Reference Field
Use the source document number as part of the transaction number to provide a cross-reference and an audit trail to allow tracing transactions to the source document that created them.

146. Correction Procedures
Clearly define procedures to be used in correcting input errors, delineating:

- The types and classes of errors that occur
- Correction procedures for error processing
- Authorization and verification procedures for generating a corrected transaction
- Logging procedures for corrected transactions
- Re-input/recycling procedures
- Balancing procedures for corrected output totals.

147. Date/Time Stamping of Source Documents
Date/time-stamp all source documents at the time of data entry to prevent multiple entries of the same transaction. Time-stamp all input transactions to avoid confusion with multiple transactions from the same source or those with similar or repetitive information.

148. Source-Data Capture
Use source-data-capture techniques that minimize both the creation and manual processing of paper transactions and opportunities for error. Methods to be considered include:

- Optical character recognition
- MICR coding
- Bar coding
- Terminal data capture at the point of origin.

149. **Verification of Input Data**
Ensure that critical data is verified for accuracy before being released for processing. This verification should be done by an operator other than the one who made the initial input, and is generally accomplished by:

- Key verification of card-input data, using independent keying of data from a source document.
- Calling up a transaction for display on a CRT, using a transaction number or other unique identifier. The verification operator then rekeys the transaction (or certain sensitive data elements) from the source document to make sure that there is a match.

150. **Transaction Identification**
Assign a unique transaction code to each transaction entered into the system.

151. **Run-to-Run Totals**
Use run-to-run totals for unit and aggregate reconciliation after each run to help prevent loss of or tampering with data between runs. Totals from each batch can be reconciled manually with the machine-generated total for the run. All out-of-balance conditions should be logged, and corrective action should be taken by supervisors.

152. **Central Control Group**
Establish a central control function responsible for all verification, error correction, re-input, and reconciliation. This function should be independent of the data entry function.

153. **Memo-Posting System**
Use memo posting for sensitive online data-capture operations. The transactions are entered online during the processing day and are batched in a transaction file. At intervals during the processing day, source documents (e.g., checks, invoices) are again input (using MICR, OCR, or the like). The two files are reconciled, and only the online transactions that match corresponding source documents are written to a live production data file.

154. **Front-End Editing of Input**
Use intelligent terminals for editing at the point of data capture. This reduces overhead on the mainframe and provides an initial level of system control. Edits that might be performed at this level include:

- Testing limits to determine whether entered values exceed predefined nominals
- Consistency checking between input data fields
- Completeness checking to ascertain that all necessary data for transaction processing has been input

- Transaction-date comparison with system clock
- Comparison between user ID/terminal ID and allowed transaction codes to ensure that the input is an authorized transaction.

155. Restricted Inputed Points
Develop both physical and programmed restrictions on terminals that process critical transactions or capture critical data (see also Countermeasures 85, 111, and 116).

156. Controlled Access to Critical Source Documents
Restrict and control access to sensitive source documents (e.g., receiving reports, vouchers, checks). Control sensitive documents with serially numbered forms.

157. Physical Control of Output
Ensure that all system output is properly controlled; controls should include the following:

- Keep all human-readable output in a physically secured area.
- Have users sign for all output received from the data center.
- Produce only enough copies to meet operational needs. Periodically review user output report requirements to ensure that excess copies or unnecessary reports are not being created.
- Reconcile actual output production with the output volume reported by the program (page-count routines).
- Destroy carbon paper after running sensitive output.
- Mark sensitive output appropriately.

See also Countermeasure 31.

158. Critical Hardware Backup
Provide backup or redundant hardware for critical system components such as CPUs, disk drives, tape drives, printers, COM units, and CRTs. These should be regularly inspected, maintained, and tested.

159. Critical Software Backup
Maintain off-site backup copies of current critical system and application software, such as:

- Operating systems
- DBMSs
- Security software
- Application software.

160. Software Modification Control
All system or application software changes should be implemented and tested on a developmental or target disk pack. After certification, this pack should be given to operators

for loading of the production system. Changes should never be made directly to a production system, and programmers should never move the change from development to production. Emergency patches made at times other than those designated for change implementation must be properly documented and reviewed by the appropriate authority within 24 hours. No changes should be made without going through the established change control/configuration management cycle (see Countermeasure 72).

SECURITY MANAGEMENT CONTROLS

161. DP Security Committee

Appoint a DP security committee to coordinate data and communications security requirements. This committee should be composed of:

- The chief operating officer
- The DP risk manager (see Countermeasure 163)
- The data security officer (see Countermeasure 164)
- The auditor
- The director of data processing
- Representatives of major system users.

This committee, which should have a written charter from the chief executive officer, should meet regularly.

162. Data Security Manual

Develop formal documentation of all DP and communications security procedures in the form of a data security manual, which should contain:

- Statement of security policy
- Organizational security responsibilities
- Data-center physical security procedures
- Online and terminal security procedures
- Security and control considerations in software development and maintenance
- Security-incident reporting procedures
- Contingency and continuity-of-operations plan, including disaster recovery and alternate-site processing.

163. DP Risk Manager/DP Security Administrator

Appoint a DP risk manager who, to maintain operational independence, reports to the individual within the organization who is responsible for overall risk management planning (e.g., corporate risk manager, controller). This person should be responsible for:

- Development of overall DP and communications security policy and standards for the organization.
- Coordination of policy implementation with the DP organization and system users.

- Conducting risk analyses of DP and communications operations and developing an overall program that integrates all aspects of risk management within the organization's automated environment, including:
  --Risk reduction and countermeasure implementation
  --Risk retention
  --Transfer of risk through insurance
- Develop contingency and continuity-of-operations plans to ensure the maintenance of essential DP and communications functions in the event of damage to or destruction of primary system resources.

At the operational level, each major user area should appoint DP security administrator to be responsible for:

- Developing (under the guidance of the risk manager) specific security operating procedures to facilitate security policy implementation within his or her area.
- Ensuring compliance with security policies and procedures within his or her area.
- Working with the risk manager to develop new policies and practices in response to changing systems and operational requirements.

164. Data Security Officer

In organizations where, size or other considerations make it infeasible to appoint a DP risk manager, a data security officer (DSO) should be appointed. For reasons of operational independence, the DSO should report outside the DP organization and should be responsible for:

- Developing DP and communications policy and procedures for all systems and users.
- Ensuring overall compliance with policies and procedures and assisting users in the resolution of security-related problems.
- Conducting risk analyses of existing and proposed systems and developing appropriate security and control postures for these systems.
- Reviewing all modifications to critical and/or sensitive systems to ensure that proper security and control has been maintained.
- Developing contingency and continuity-of-operations plans.

SOURCE: Ref. 26: pp. II-A-1 to II-A-27.

APPENDIX J

THREATS/ASSETS/CONTROLS MATRIX

Assets	Threats	Controls
1.1	A.1	8, 9, 10, 25, 27, 36, 39, 161-64
	A.2	8, 9, 24, 25, 26, 27, 36, 39, 161-64
	A.3	4, 5, 7, 8, 9, 23, 36, 39, 161-64
	A.4	4, 5, 7-10, 23, 36, 51, 161-64
	A.5	8, 9, 36, 39, 161-64
	A.6	8, 9, 36, 39, 161-64
	A.7	8, 9, 36, 39, 161-64
	B.9	8, 9, 35, 39, 161-64
	B.10	8, 9, 35, 161-64
	C.3	1, 2, 8, 9, 12, 14, 16, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	8, 9, 161-64
	D.1	1, 2, 8, 9, 12, 28, 32, 33, 35, 36, 161-64
1.2	A.1	6-8, 15, 20, 21, 27, 36, 161-64
	A.2	6-8, 20, 25, 26, 27, 36, 161-64
	A.3	4, 5, 7, 20, 36, 161-64
	A.4	4, 5, 7, 20, 21, 22, 36, 161-64
	A.7	6, 36, 161-64
	B.1	6, 36, 39, 161-64
	C.3	1, 2, 12, 18, 19, 28, 29, 32, 33, 35, 36, 39, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
1.3	A.1	6, 8, 11, 15, 25-27, 36, 161-64
	A.2	6, 8, 11, 25, 26-27, 36, 161-64
	A.3	4, 5, 11, 36, 161-64
	A.4	4, 5, 11, 22, 36, 161-64
	A.5	11, 36, 161-64
	A.6	11, 36, 161-64
	A.7	11, 36, 161-64
	B.1	6, 11, 36, 161-64
	B.2	11, 15, 36, 39, 161-64
	C.3	1, 2, 12, 18, 19, 28, 29, 32, 33, 35, 36, 39, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
1.4	A.1	36, 161-64
	A.2	36, 161-64

	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.1	6, 36, 161-64
	C.3	28, 29, 32, 33, 35, 36, 39, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
1.5	A.1	36, 161-64
	A.2	36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.1	6, 36, 161-64
	C.3	28, 29, 32, 33, 35, 36, 38, 39, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 38, 161-64
2.1	A.1	8, 15, 24-27, 36, 161-64
	A.2	8, 25-27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	A.5	37, 161-64
	B.1	6, 36, 53, 161-64
	B.6	36, 39, 158, 161-64
	B.9	3, 39, 39, 161-64
	B.10	66, 67, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
	D.3	54-65, 161-64
	D.4	1, 2, 12, 28, 29, 32, 33, 35, 36, 161-64
2.2	A.1	8, 15, 24, 25, 26, 27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	A.5	37, 161-64
	B.1	6, 13, 36, 161-64
	B.6	36, 39, 158, 161-64
	B.9	3, 35, 39, 161-64
	B.10	66, 67, 161-64
	C.3	1, 1, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36
2.3	A.1	8, 15, 24-27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64

	B.1	6, 13, 36, 161-64
	B.6	36, 39, 158, 161-64
	B.10	66, 67, 161-64
	C.2	115, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
	D.3	108-124, 161-64
	D.5	108-124, 161-64
2.4	A.1	8, 15, 24, 25, 26, 27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	A.5	37, 161-64
	B.1	6, 13, 36, 161-64
	B.3	132, 161-64
	B.4	36, 39, 125, 136, 161-64
	B.5	125, 161-64
	B.10	66, 67, 161-64
	C.2	115, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 134, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
	D.3	128, 161-64
	D.4	1, 2, 12, 28, 29, 32, 33, 35, 36, 161-64
	D.5	128, 161-64
2.5	A.1	8, 15, 24, 25, 26, 27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	A.5	37, 161-64
	B.1	6, 13, 36, 161-64
	B.3	131, 132, 133, 161-64
	B.4	36, 39, 125, 136, 161-64
	B.10	66, 67, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 161-64
	D.1	1, 2, 12, 28, 32-33, 35, 36, 161-64
2.6	A.1	8, 15, 24, 25, 26, 27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	B.1	6, 36, 161-64
	B.3	132, 161-64
	B.4	36, 39, 125, 136, 161-64

	B.5	125, 161-64
	B.10	66, 67, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
2.7	A.1	8, 15, 24-27, 36, 161-64
	A.2	8, 25-27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	B.1	6, 36, 161-64
	B.3	132, 161-64
	B.4	36, 39, 125, 136, 161-64
	B.10	66-67, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35-36, 39, 161-64
	C.4	4, 5, 36, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
2.8	A.1	8, 15, 24, 25, 26, 27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	B.1	6, 36, 161-64
	B.3	125, 126, 132, 161-64
	B.4	125, 136, 161-64
	B.5	125, 161-64
	B.6	36, 39, 158, 161-64
	B.10	66, 67, 161-64
	C.2	115, 124, 161-64
	C.3	1, 2, 12, 14, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 121, 122, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
	D.3	90, 108-124, 127, 155, 161-64
	D.4	1, 2, 12, 28, 29, 32, 33, 35, 36, 161-64
	D.5	90, 108-124, 127, 155, 161-64
2.9	A.1	8, 15, 24, 25, 26, 27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	B.1	6, 36, 161-64
	B.3	132, 161-64
	B.4	36, 39, 125, 136, 161-64
	B.10	66, 67, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 6, 63, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64

2.10	A.1	8, 15, 24, 25, 26, 27, 36, 161-64
	A.2	8, 25, 26, 27, 36, 161-64
	A.3	4, 5, 36, 161-64
	A.4	4, 5, 22, 36, 161-64
	B.1	6, 36, 161-64
	B.3	132, 161-64
	B.4	36, 39, 125, 136, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
2.11	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.3	36, 39, 125, 126, 129, 130, 132, 161-64
	B.9	3, 39, 161-64
	C.2	114, 115, 120, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 36, 39, 118, 119, 123, 161-64
	C.4	4, 5, 36, 121, 122, 135, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
	D.3	114, 118, 119, 135, 161-64
	D.5	118, 119, 120, 161-64
2.12	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.3	36, 39, 125, 126, 129, 120, 132, 137, 161-64
	B.9	3, 39, 161-64
	C.2	114, 115, 120, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 121, 122, 135, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
	D.3	114, 135, 161-64
	D.5	114, 120, 161-64
2.13	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.3	36, 39, 125, 126, 129, 130, 132, 137, 161-64
	B.9	3, 39, 161-64
	C.2	114, 115, 120, 161-64
	C.3	1, 2, 12, 28, 29, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 36, 121, 122, 135, 161-64
	D.1	1, 2, 12, 28, 32, 33, 35, 36, 161-64
	D.3	114, 135, 161-64
	D.5	114, 120, 161-64

3.1	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.7	36, 39, 68-78, 82-103, 159, 161-64
	B.9	3, 39, 161-64
	C.3	28, 29, 30, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 30, 36, 68-78, 161-64
	D.2	1, 2, 12, 28, 30, 32, 33, 35, 36, 161-64
	D.3	54-65, 82-103, 109, 161-64
	D.4	1, 2, 12, 28, 29, 30, 32, 33, 35, 36, 79, 161-64
3.2	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.7	36, 39, 68-78, 82-107, 159, 161-64
	B.9	3, 39, 161-64
	C.3	28, 29, 30, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 30, 36, 68-78, 161-64
	D.2	1, 2, 12, 28, 30, 32, 33, 35, 36, 161-64
	D.3	54, 82-107, 109, 161-64
	D.4	1, 2, 12, 28, 29, 30, 32, 33, 35, 36, 79, 161-64
3.3	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.5	36, 39, 68-78, 82-103, 138, 161-64
	B.9	3, 39, 161-64
	C.3	28, 29, 30, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 30, 36, 68-78, 138, 161-64
	D.2	1, 2, 12, 28, 30, 32, 33, 35, 36, 138, 161-64
	D.3	82-103, 161-64
	D.4	1, 2, 12, 28, 30, 32, 33, 35, 36, 79, 161-64
3.4	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.7	36, 39, 68-78, 82-103, 159, 161-64
	B.9	3, 39, 161-64
	C.3	28, 29, 30, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 30, 36, 161-64
	D.2	1, 2, 12, 28, 30, 32, 33, 35, 36, 161-64
	D.3	79, 109, 161-64
	D.4	1, 2, 12, 28-30, 32, 33, 35, 36, 79,

		161-64
3.5	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	B.8	36, 39, 68-78, 82-103, 159, 161-64
	B.9	3, 39, 161-64
	C.1	153, 154, 161-64
	C.3	28, 29, 30, 32, 33, 35, 36, 39, 161-64
	C.4	4, 5, 30, 36, 68-78, 161-64
	D.2	1, 2, 12, 28, 30, 32, 33, 35, 36, 161-64
	D.3	54, 82-103, 161-64
	D.4	1, 2, 12, 28-30, 32, 33, 35, 36, 79, 161-64
	D.5	153, 154, 161-64
4.1	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.1	36, 139-152, 154, 161-64
	C.2	32, 35, 36, 40, 68-78, 80, 81, 155-157, 161-64
	C.3	1, 2, 12, 28, 29-39, 156, 161-64
	C.4	4, 5, 30, 36, 68-78, 161-64
	D.2	1, 2, 12, 28, 30, 32, 33, 34, 35, 36, 161-64
	D.3	35, 36, 68-78, 79, 80, 81, 161-64
	D.5	30, 34, 35, 79, 81, 139-52, 156, 161-64
4.2	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.1	36, 139-52, 154, 161-64
	C.2	31, 35, 36, 40, 68-78, 80, 81, 155-57, 161-64
	C.3	1, 2, 12, 28-36, 39, 156, 161-64
	C.4	4, 5, 30, 36, 68-78, 161-64
	D.2	1, 2, 12, 28, 30, 32-36, 161-64
	D.3	35, 36, 68-81, 161-64
	D.5	30, 34, 35, 79, 81, 139-52, 156, 161-64
4.3	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.1	36, 139-52, 154, 161-64
	C.2	32, 35, 36, 40, 68-78, 80, 81, 155-157, 161-64
	C.3	1, 2, 12, 28-36, 39, 156, 161-64
	C.4	4, 5, 30, 36, 68-78, 161-64
	D.2	1, 2, 12, 28, 30, 32-36, 161-64
	D.3	35, 36, 68-81, 161-64
	D.5	30, 34, 35, 79, 81, 139-52, 156,

		161-64
5.1	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.2	36, 41-43, 46-48, 161-64
	C.3	14, 161-64
	C.4	46, 161-64
	D.1	46, 161-64
	D.2	46, 47, 161-64
	D.4	46, 47, 161-64
	D.5	36, 42, 46
5.2	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.1	36, 46, 139-52, 161-64
	C.2	12, 36, 41-43, 46-48, 161-64
	C.3	14, 161-64
	C.4	46, 161-64
	D.1	46, 47, 161-64
	D.2	46, 47, 161-64
	D.5	12, 36, 42, 44-47, 49-52, 139-52, 161-64
5.3	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.2	12, 36, 42-43, 46-48, 161-64
	C.3	14, 161-64
	C.4	46, 161-64
	D.1	46, 47, 161-64
	D.2	46, 47, 161-64
	D.5	36, 42, 46, 47, 49-52, 161-64
5.4	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.2	36, 41-43, 46-48, 161-64
	C.3	14, 161-64
	C.4	46, 161-64
	D.1	46, 47, 161-64
	D.2	46, 47, 161-64
	D.4	46, 47, 161-64
	D.5	36, 42, 45-47, 49-52, 160-64
5.5	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.1	36, 41-43, 46-48, 161-64
	C.3	14, 161-64
	C.4	46, 161-64
	D.1	46, 47, 161-64
	D.2	46, 47, 161-64
	D.4	46, 47, 161-64
	D.5	36, 42, 45-47, 49-52, 160-64

5.6	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.2	36, 42-43, 46-48, 161-64
	C.3	14, 161-64
	C.4	46, 161-64
	D.1	46, 47, 161-64
	D.2	46, 47, 161-64
	D.5	36, 42, 46, 47, 49-52, 161-64
5.7	A.3	4, 5, 36, 161-64
	A.4	4, 5, 36, 161-64
	C.2	36, 41-43, 46-48, 161-64
	C.3	14, 161-64
	C.4	46, 161-64
	D.1	46, 47, 161-64
	D.2	46, 47, 161-64
	D.5	36, 42, 46, 47, 49-52, 161-64

SOURCE: Ref. 26: p. II-4-5.

APPENDIX K

CONTROLS APPLICABILITY BY SENSITIVITY/CRITICALNESS LEVEL

Controls	A	B	C	D	E	F	G	H	I	J	K	L
1.1	X	X	X	X								
1.2	X	X	X									
1.3	X	X										
1.4	X	X										
2.1	X	X	X	X								
2.2	X	X	X	X								
2.3	X	X	X	X								
2.5	X	X	X	X	X							
2.6	X	X	X	X								
3.1							X	X	X	X	X	
3.2							X	X	X	X	X	
3.3							X	X	X	X	X	X
4.1							X	X	X	X	X	X
4.2							X	X	X	X	X	X
5.1											X	X
5.2							X	X	X	X	X	X
5.3										X	X	X
5.4												X
6.							X	X				
7.							X	X	X	X	X	X
8.	X	X					X	X	X	X		
9.							X	X	X			
10.							X	X	X	X	X	X
11.							X	X	X	X	X	X
12.	X	X	X	X								
13.							X	X	X	X	X	
14.	X	X	X	X								
15.	X	X	X	X								
16.	X	X	X									
17.							X	X	X	X		
18.							X	X	X	X		
19.							X	X	X	X		
20.							X	X	X	X	X	X
21.							X	X	X	X	X	X
22.							X	X	X	X	X	X
23.							X	X	X	X	X	X
24.							X	X	X	X	X	X
25.							X	X	X	X	X	X
26							X	X	X	X	X	X
27.							X	X	X	X	X	X
28.												
28.1	X	X	X	X								

Controls	A	B	C	D	E	F	G	H	I	J	K	L
28.2	X	X	X	X								
28.3	X	X	X									
29.												
29.1	X	X										
29.2	X	X	X	X								
30.	X	X	X	X			X	X	X	X		
31.	X	X	X	X								
32.	X	X	X	X								
33.	X	X	X	X								
34.							X	X	X	X	X	X
34.1							X	X	X	X	X	X
34.2	X	X	X	X								
34.3	X	X	X	X	X	X						
35.	X	X	X	X	X							
36.	X	X	X	X	X	X	X	X	X	X	X	X
37.							X	X	X	X		
38.	X	X	X	X								
39.							X	X	X	X	X	X
40.	X	X	X	X	X							
41.	X	X	X	X								
42.	X	X	X									
43.	X	X	X	X	X							
44.	X	X										
45.	X	X	X	X								
46.	X	X	X	X	X	X						
47.	X	X	X	X	X	X						
48.	X	X	X	X	X	X						
49.	X	X	X	X								
50.	X	X	X	X								
51.	X	X	X									
52.	X											
53.							X	X	X	X	X	X
54.	X	X	X	X								
55.	X	X	X	X								
56.	X	X	X	X	X	X						
57.	X	X										
58.	X	X										
59.	X	X	X	X	X	X						
60.	X	X	X	X								
61.	X	X	X	X								
62.	X	X	X	X								
63.	X	X	X	X								
64.	X	X	X	X	X	X						
65.	X	X										
66.	X	X										
67.	X	X										
68.	X	X	X	X	X	X	X					
69.	X	X	X	X	X	X	X					
70.	X	X	X	X	X	X	X					
71.	X	X	X	X	X	X	X					

Controls	A	B	C	D	E	F	G	H	I	J	K	L
72.	X	X	X	X	X	X						
73.	X	X	X									
74.	X	X	X	X	X	X						
75.	X	X	X	X	X	X						
76.	X	X	X	X	X	X						
77.	X	X	X	X								
78.	X	X	X	X	X	X						
79.	X	X	X	X								
80.	X	X	X	X								
81.	X	X										
82.	X	X										
83.	X	X	X									
84.	X	X	X									
85.	X	X	X	X								
86.	X	X										
87.	X	X	X	X								
88.	X	X	X	X	X							
89.	X	X	X									
90.	X	X	X	X								
91.	X	X	X	X	X	X						
92.	X	X	X	X	X	X						
93.	X	X	X	X	X	X						
94.	X	X	X	X	X	X						
95.	X	X	X									
96.	X	X	X									
97.	X	X	X	X	X	X						
98.	X	X	X	X	X	X						
99.	X	X	X	X	X	X						
100.	X	X	X	X	X	X						
101.							X	X	X	X	X	X
102.	X	X	X	X	X	X						
103.	X	X	X	X	X	X						
104.	X	X	X	X								
105.	X	X	X									
106.							X	X	X	X		
107.							X	X	X	X	X	X
108.	X	X	X									
109.	X	X	X	X	X							
110.	X	X	X	X	X							
111.	X	X	X	X								
112.	X	X	X	X								
113.	X	X	X	X								
114.	X	X	X									
115.	X	X										
116.	X	X	X	X								
117.	X	X										
118.	X	X										
119.	X	X										
120.	X	X	X									
121.	X	X	X	X	X							

Controls	A	B	C	D	E	F	G	H	I	J	K	L
122.	X	X	X	X	X							
123.	X	X	X	X								
124.	X	X	X	X								
125.	X	X	X	X	X	X						
126.							X	X	X	X		
127.	X	X	X	X								
128.	X	X	X									
129.	X	X	X	X	X	X						
130.							X	X	X	X		
131.							X	X	X	X		
132.							X	X	X	X		
133.							X	X	X	X		
134.							X	X	X	X	X	X
135.	X	X	X	X	X	X	X	X	X	X	X	X
136.							X	X	X			
137.							X	X	X			
138.							X	X	X	X	X	X
139.	X	X	X	X	X							
140.	X	X	X	X								
141.	X	X	X	X	X	X						
142.	X	X	X	X	X							
143.	X	X	X	X								
144.	X	X	X	X								
145.	X	X	X	X								
146.	X	X	X	X	X	X						
147.	X	X	X	X								
148.	X	X	X	X	X	X						
149.	X	X	X	X	X	X						
150.	X	X	X	X	X	X						
151.	X	X	X	X	X	X	X	X	X	X	X	X
152.	X	X	X	X	X	X						
153.	X	X	X									
154.	X	X	X	X								
155.	X	X	X	X								
156.	X	X	X	X								
157.	X	X	X									
158.							X	X	X	X		
159.							X	X	X	X		
160.	X	X	X	X	X	X						
161.	X	X	X	X	X	X						
162.	X	X	X	X	X	X						
163.	X	X	X	X	X	X						
164.	X	X	X	X	X	X						

SOURCE: Ref. 26: pp. I-E-6 to I-E-10.

APPENDIX L

SECURITY DATABASE CONTENTS

- Security policy information
- Security-related laws and regulations information
- Top management security needs and concerns information
- IS objectives and measures of performance information
- Identified and defined IS users information
- Users' security needs and concerns information
- IS components (tasks) information
- IS configuration information
- IS plans information
- Applications under development information
- Existing IS applications information
- IS security-related policy statements, standards, rules, procedures and guidelines information
- Results of audits and inspections information
- History of security violations and problems information
- Applications, data, and transactions classification information
- Threats inventory information
- Impact analysis information
- Vulnerability assessment information
- Logical design information
- Practical design information
- Testing information

- Security configuration information
- Security budgetary and staff information
- Security staff procedures, standards, rules, and policies.

LIST OF REFERENCES

1. Friedrich, Otto, "The Computer Moves In," Time, pp. 14-24, January 3, 1983.

2. Nolan, Richard L., "Managing the Crisis in Data Processing," Harvard Business Review, pp. 115-126, March-April 1979.

3. Cash, James I., Jr., McFarlan, F. Warren, and McKenney, James L., Corporate Information Systems Management--Text and Cases, Richard D. Irwin, Inc., 1983.

4. Clemons, Eric K., "When does DP Give the Edge?" Computerworld, pp. 65, 70, & 73, July 28, 1986.

5. Friedberg, Dr. Alan H. and Harper, Robert M., Jr., "Electronic Media Data Retention in an Environment of Change," The EDP Auditor Journal, pp. 24-32, Vol. III, 1986.

6. Elmer-DeWitt, Philip, "Networking the Nation," Time, pp. 38-39, June 16, 1986.

7. Seligman, Daniel, "Life Will Be Different When We're All On-Line," Fortune, pp. 68-72, February 4, 1985.

8. Naisbitt, John, Megatrends, Warner Communications Company, 1984.

9. Bequai, August, "Computer Snafus Keep Govt. In High-Tech Dark Ages," Government Computer News, p. 52, June 20, 1986.

10. Fredell, Eric, "Agency Data Linking Said To Conflict With Privacy Act," Government Computer News, p. 4, July 18, 1986.

11. Sanders, Donald H., Computers Today, McGraw-Hill Book Company, Inc., 1983.

12. Parker, Donn B., Fighting Computer Crime, Charles Scribner's Sons, 1983.

13. Horwitt, Elisabeth, "Service Lets Multinational Access Overseas Applications," Computerworld, p. 2, July 7, 1986.

14. Tlustos, Chris, "Courts Show Transcripts in Real Time," Government Computer News, pp. 1 & 22, August 1, 1986.

15. Bowen, Ezra, "New Paths to Buried Treasure," Time, p. 56, July 7, 1986.

16. Sullivan, Judith A., "Computers Saving Lives in Hurricane Season," Government Computer News, pp. 3 & 5, September 27, 1985.

17. Koepp, Stephen, "The Boss That Never Blinks," Time, p. 46, July 28, 1986.

18. "Living: Pushbutton Power," Time, pp. 46-49, February 20, 1978.

19. Thompson, Larry, "Hospital Computer Advises Doctors in Giving Treatment," The Philadelphia Inquirer, November 22, 1984.

20. Coy, Peter, "Firms Guard Against Computer Wipeouts," The Sunday Peninsula Herald, p. 10A, January 19, 1986.

21. Koshetz, Charles and Petruno, Tom, "Computers Underlie Big Stock Moves," USA Today, pp. 1B-2B, January 10, 1986.

22. Dentzer, Susan, "Greed on Wall Street," Newsweek, pp. 44-46, May 20, 1986.

23. Elmer-DeWitt, Philip, "An Electronic Assault on Privacy?" Time, p. 104, May 19, 1986.

24. Betts, Mitch, "Privacy Threat Seen by an Agency," Computerworld, pp. 1 & 14, July 7, 1986.

25. Sherizen, Sanford and Marx, Gary, "Technology: Invader or Protector of Privacy?" Computerworld, pp. 59-64, July 28, 1986.

26. Elmer-DeWitt, Philip, "The Granite State of the Art," Time, p. 70, January 27, 1986.

27. Edwards, Robert W. and Edwards, Lynda E., Data Processing Security and Control Practices and Methodologies, Auerbach Publishers, Inc., 1984.

28. Sandza, Richard, "Spying Through Computers," Newsweek, p. 39, June 10, 1985.

29. Churchman, C. West, The Systems Approach, Delacorte Press, 1968.

30. Smith, Fred and Cook, Virgil G., "A Model for Influencing and Managing Change," 1986.

31. Ein-Dor, Phillip and Jones, Carl R., Information Systems Management: Analytical Tools and Techniques, Elsevier Publishing Company, Inc., 1985.

32. Hamilton, Scott and Chervany, Norman L., "Evaluating Information System Effectiveness--Part I: Comparing Evaluation Approaches," MIS Quarterly, pp. 55-69, September 1981.

33. Kroenke, David M., Business Computer Systems--An Introduction, Second Edition, Mitchell Publishing Company, Inc., 1984.

34. Champine, George A., Distributed Computer Systems--Impact on Management, Design, and Analysis, North-Holland Publishing Company, 1980.

35. Parker, Donn B., Computer Security Management, Reston Publishing Company, Inc., 1981.

36. Karabin, Stephen J., "Data Classification for Security and Control," EDPACS--The EDP Audit, Control and Security Newsletter, pp. 1-20, Vol. XIII, No. 6, December 1985.

37. Wilkin, Barry J., The Internal Auditor's Information Security Handbook, The Institute of Internal Auditors, Inc., 1979.

38. Blalock, Hubert M., and Blalock, Ann B., Methodology in Social Research, McGraw-Hill Book Company, 1968.

39. Pollack, Bill, "Defining Security Requirements is a Six-Step Job," Government Computer News, pp. 64, 68-69, June 20, 1986.

40. Department of the Navy, OPNAV Instruction 5239.1A, Department of the Navy Automatic Data Processing Security Program, 3 August 1982.

41. National Bureau of Standards (NBS), U.S. Department of Commerce, "Guidelines for Automatic Data Processing Risk Analysis," Federal Information Processing Standards (FIPS) Publication 65, 1979 August 1 Computer Security Handbook, Computer Security Institute, 1985.

42. Betts, Mitch, "Computer Crime Bill Passed with Tough Jail Terms for Offenders," Computerworld, Vol. XX, No. 41, October 13, 1986.

43. Bruu, Lois, "Some Countries Set Limits on Data Crossing Borders," Management Information Week, Vol. 7, No. 40, October 6, 1986.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Defense Logistics Studies Information Exchange (DLSIE) U.S. Army Logistics Management Center Fort Lee, Virginia 23801-6043	1
4.	Professor James M. Fremgen, Code 54Fm Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
5.	Adjunct Professor Michael P. Spencer, Code 54Sp Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1
6.	Mr. Joseph George Boyce Naval Audit Service Capital Region 1941 Jefferson Davis Highway Crystal Mall, Room 325 Washington, D.C. 20376	1

Thesis
B7837 Boyce
c.1 A model for the development of an organization's information system (IS) security system.